现代应用数学手册

《现代应用数学手册》编委会

离散数学卷

清华大学出版社

33

《现代应用数学手册》编委会

现代应用数学手册

离散数学卷



清华大学出版社

(京)新登字 158 号

内 容 简 介

本书介绍离散数学最核心的部分：集合论，组合数学与图论，代数结构与泛代数，标准（古典）与非标准（非古典）数理逻辑．书中从理论与应用方面深入浅出地阐述各分支中的基本概念，基本理论与基本方法．注重背景，强调应用，便于读者加深理解、掌握与应用．本书可供理、工、医、农、经管等各个领域中的广大科技人员，大、中专院校教师、学生、研究生使用．

书　名：现代应用数学手册（离散数学卷）
作　者：《现代应用数学手册》编委会
出版者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
http：//www. tup. tsinghua. edu. cn
印刷者：清华大学印刷厂
发行者：新华书店总店北京发行所
开　本：850×1168 1/32　印张：21　字数：498 千字
版　次：2002 年 3 月第 1 版　2002 年 3 月第 1 次印刷
书　号：ISBN 7-302-04565-8/O・260
印　数：0001～2000
定　价：33.00 元

《现代应用数学手册》
编 辑 委 员 会



离散数学卷

责任编委　马振华

章次	编者	校者
1～6	马振华	李忠傧
7～13	胡冠章	王殿军
14～16	李忠傧	马振华，马连荣
17～18	李忠傧	马振华
19～20	李忠傧，袁健	马振华
21～23	马振华	李忠傧



序

随着计算机科学技术的飞速发展，人类正进入信息时代.

信息时代是应用数学大发展的时代，人类长期积累起来的知识体系，正面临着第3次数学化. 数学思想，数学方法与数学模型随着计算机的广泛应用，日益渗透到各种行业中去.

当代，除了古典的数学理论（初等数学，微积分学，微分方程，复变函数等）早已得到广泛的应用外，一些比较抽象的现代数学理论（集合论、数理逻辑、范畴论、抽象代数、泛代数、代数几何、拓扑学、泛函分析等）以及一些新兴的数学理论（随机过程、时间序列、运筹学、最优化理论、有限元方法、模糊数学、混沌与分形等）也逐渐地成为社会生产、科学实验、工程技术及经济管理中不可缺少的工具，应用数学的适用范围正在迅速地扩大.

为了满足日益增长的社会需求，清华大学应用数学系《现代应用数学手册》编委会，组织编写了这套多卷集的手册.

本书读者是理、工、医、农、经管等各个领域中的广大工程技术人员、科研人员、大、中专院校的教师、学生、研究生及其他使用数学工具的实际工作者. 其中有些内容对于中学生也是适用的.

编者力求使本书成为一套高质量的工具书，它有下列特点：

(1) **内容“新颖”** 本书力求做到内容现代化，除用现代观点介绍古典内容外，对已出现的新理论、新方法尽量优先选入.

(2) **突出“应用”** 本书在选材上突出数学理论的应用，以通俗易懂的方式着重介绍在现代科学技术等实际领域中应用广泛的数学理论和方法.

(3) **紧密“结合”计算机应用** 为了更有效地应用数学方法解

决各种实际问题，广大科技人员迫切要求数学方法与计算机应用相结合，提高工作效率. 为此，本书在结合计算机应用方面，给予特别的重视.

(4) **版面设计"合理"，便于迅速查阅** 为方便读者使用，本书采用了一套较为完善的索引体系. 除正文中章、节的编号沿用国际通行的十进制编号外，对于重要的定义、定理、例题、公式、图、表等均有编号. 读者可以从(1) 目录，(2) 中文—外文索引，(3) 外文—中文索引等三种途径，迅速找到所需资料. 此外，本书对载入的外国科学家人名，尽量采用"名从主人"的原则.

(5) **数学符号力求"统一"与国际化** 鉴于目前国内各种文献、书籍中使用的数学符号不够统一与国际化，增加了读者阅读时的困难. 本书除按国家标准 GB3102—93 外，兼用国际数学界权威著作《数学大百科辞典》(Encyclopedic Dictionary of Mathematics, EDM)中的符号为标准. 对于不在上述文献中的其他新符号，则选用较为流行者.

本手册各卷内容独立完整，便于个人读者与团体读者按需选购. 当前应用数学急剧发展，编委会在条件成熟的时候，还将增出新卷.

本书的编撰是与清华大学应用数学系领导，特别是萧树铁教授的热心支持，编辑委员会各位编委的通力协作，校内外的许多教师、科研工作者的大力支持分不开的，编者深致谢意.

在编辑出版过程中，还得到清华大学出版社的热情支持.

本书从编撰到出版，历尽艰辛，饮水思源，编者还要感谢本书的发起人，清华大学应用数学系陆璇教授，北京出版社李利军编辑及已故的北京出版社社长王政人先生.

最后，编者还要对夫人王华敏表示谢忱，没有她的深刻理解、热情支持与持久的帮助，本书也难以问世.

主编　马振华

1997 年于清华园

符 号 表

符号	含义
∀	全称量词
∃	存在量词
$\vdash(\vdash_L \mathscr{A})$	断定符(公式$\mathscr{A}$在L中可证)
$\models(\models_E \mathscr{A})$	满足符(公式$\mathscr{A}$在E上有效,公式$\mathscr{A}$在E上可满足)
¬(~,¯, NOT)	命题的“非”运算
∧(&, AND)	命题的“合取”(“与”)运算
∨(OR)	命题的“析取”(“或”,“可兼或”)运算
→(⇒,IF…THEN…)	命题的“蕴含”运算
↔(≡, iff)	命题的“等价”运算
$\overline{\vee}$($\underline{\vee}$)	命题的“不可兼或”运算(“异或门”)
↑(|, NAND)	sheffer 竖(“与非门”)
↓(NOR)	pierce 箭(“或非门”)
□(L)	模态词“必然”
◇(M)	模态词“可能”
∅	空集
∈	属于($\notin$,$\bar{\in}$不属于)
$\mu_A(\cdot)$	集A的特征函数(隶属函数)
$\mathscr{P}(A)$	集A的幂集
$\underbrace{A\times A\times\cdots\times A}_{n}$($^nA$, A^n)	集合A的笛卡儿积
$R^2=R\circ R(R^n=R^{n-1}\circ R)$	关系R的“复合”
$\aleph_0$	阿列夫零

$\aleph_1(\aleph)$　阿列夫

$\supseteq$　包含

$\supset$　真包含

$\cup$　集合的并运算

$\cap$　集合的交运算

$\setminus$　集合的差运算

$\dot{-}(\triangle, \dot{+}, \oplus)$　集合的“对称差”(Minkowski 和)

$\oplus$　对位 Boole 和(直和)

$\upharpoonright$　限制

$+_m$　m 同余加

$[x]_R$　集合关于关系 R 的等价类

A/R　集合 A 上关于 R 的商集

$\pi_R(A)$　集合 A 关于关系 R 的划分

$R_\pi(A)$　集合 A 关于划分 π 的关系

(a)　主理想

$\langle a\rangle$　循环群

$\boldsymbol{I}$　理想,环

$\mathbf{Z}/(n)$　模 n 的同余类集

$\boldsymbol{H}_{i\cdot}$　矩阵 $\boldsymbol{H}$ 的第 i 个行向量

$\boldsymbol{H}_{\cdot j}$　矩阵 $\boldsymbol{H}$ 的第 j 个列向量

$\hom(R^{(m)}, R^{(n)})$　$R^{(m)}$ 到 $R^{(n)}$ 的模同态

$[XY]=XY-YX$　交换子乘积

$h_{\mathscr{C}}(A,B)$　态射(箭)

$h_{\mathscr{C}}(A,—)$　由 $\mathscr{C}$ 中对象 A 确定的(共变)函子

$\operatorname{ann} x$　x 的零化子(x 的阶理想)

CP　演绎定理

EG　存在推广规则

ES　存在特指规则

UG　全称推广规则

US　全称特指规则

I_A，R°　恒等关系

$\overline{A}$，A'　集合 A 的补集

X^X，${}^XX$　所有 X 到自身的映射

$\overline{\overline{M}}$，$|M|$　集合 M 的势（基数）

R　关系

$\not R$　否关系

$\bar{R}$　补关系

R^{-1}　逆关系

R^+，$t(R)$　关系 R 的传递闭包

R^*，$rt(R)$　关系 R 的自反、传递闭包

$R\circ S$　关系 R 与关系 S 的复合

$\underbrace{R\circ\cdots\circ R}_{n}$，$R^n$　关系 R 的 n 次幂

$r(R)$　关系 R 的自反闭包

$s(R)$　关系 R 的对称闭包

$t(R)$　关系 R 的传递闭包

$\underbrace{B_2\times\cdots\times B_2}_{r}$，$B_2^r$　布尔代数 B_2 的 r 次积

B_{2^r}　含有 2^r 个元素的布尔代数

$\mathscr{A}$，$\mathscr{B}$，$\mathscr{C}$　合式公式

$\binom{n}{k}$　二项式系数

$\binom{n}{n_1, n_2, \cdots, n_p}$　多项式系数

$[1,n]$　1 到 n 的整数集合

$[x]_k=x(x-1)\cdots(x-k+1)$

$[x]^k=x(x+1)\cdots(x+k-1)$

$[x|\alpha]_n=(x-a_0)(x-a_1)\cdots(x-a_{n-1}),[x|\alpha]_0=1$

$\alpha=(a_0,a_1,a_2,\cdots)$

$\begin{bmatrix} n \\ k \end{bmatrix}_q$ Gauss 系数

$C(n,k)$ 组合数

$d(u,v)$ 点 u 与点 v 间的距离

$d(v)$ 点 v 的次(度)

$d^+(v)$ 点 v 的出次(度)

$d^-(v)$ 点 v 的入次(度)

$E(n,m,k)$ 实际依赖于所有变量的函数的个数

$G=(V,E)$ 图

G^* 平面图 G 的对偶图

K_n n 阶完全图

$K_{n,m}$ 完全二分图

$L_N(t_1^{m_1}\times t_2^{m_2}\times\cdots\times t_k^{m_k})$ 正交试验表

$OA(n,m)$ 正交表

$p(n|h)$ n 的所有分拆中最小部分为 h 的分拆数

$p(n,m|h)$ 整数 n 分为 m 部分,最小部分为 h 的分拆数

$p(G;t_1,t_2,\cdots,t_n)/Z(G;t_1,t_2,\cdots,t_n)$ 群 G 的循环指标

$r(k,l)$, $r(k_1,k_2,\cdots,k_m)$, $r(q_1,q_2,\cdots,q_n,t)$ Ramsey 数

S_n n 次对称群

$S_n^{(2)}$ n 次二元对称群

$S(n,k)$ 第二类 Stirling 数

$s(n,k)$ 第一类 Stirling 数

$S_a(n,k)$ 推广的第二类 Stirling 数

$s_a(n,k)$ 推广的第一类 Stirling 数

$Z(G;t_1,\cdots,t_n)$ 群 G 的轮换指标

$\alpha(G)$ 图 G 的独立数

$\alpha'(G)$ 图 G 的边独立数

$\mu(x,y)$, $\mu(d,n)$, $\mu(n)$ Möbius 函数

$\varphi(n)$ Euler 函数

C 复数集

N 自然数集(包括 0 在内)

$\mathbf{N}^{+}$ 正自然数集

P 素数集

Q 有理数集

$\mathbf{Q}^{+}$ 正有理数集

$\mathbf{Q}^{-}$ 负有理数集

R 实数集

Z 整数集

$\mathbf{Z}_m$ $\{[1],[2],\cdots,[m]\}$

$\mathbf{Z}_p$ p 进整数环

Set 集范畴

Top 拓扑空间范畴

Ab 交换群范畴

Grp 群范畴

Mon 单元半群范畴

Ring 有单位元的(结合)环范畴

Rng 环范畴

CRng 交换环范畴

R-**mod** 环 R 的左模范畴

mod-R 环 R 的右模范畴

Field 域范畴

Poset 偏序集范畴

Ω-**Alg** Ω 代数范畴

目　　录

组合学与图论

代数结构与泛代数

数理逻辑

集　合　论

1　基本概念

1.1　引言

什么是集合？集合就在我们身边．人们在研究客观世界的各种事物时，常常把具有某种特性的事物汇集在一起，看做是一个"整体"，例如"全体中国人"．这样的"整体"就叫做集合．

客观事物的"特性"是极其复杂的．如何根据"特性"来确定集合并非总是轻而易举的．从数学上给出严格的定义也绝非易事，稍不留神还会产生种种"悖论"．

"集合"概念，类似于欧氏几何学中的"点"，"线"，"面"诸概念．我们先从直观入手，概括出描述性的定义，然后再介绍公理集合论．

1.2　集合的古典定义

由集合论创始人 G. Cantor 所给出．

定义 1.2.1　凡是在人们的感知或思维中可以明确区分的对象物，把它看成是一个整体，这个整体就称作**集合**(set)．

集合中的"对象物"称为该集合中的"成员"或"元素"

(element).

元素 a 在集合 S 中表示为 $a\in S$. 元素 a 不在集合 S 中表示为 $a\notin S$(或 $a\overline{\in}S$). 其中符号"$\in$"表示"属于"关系.

通常用大写拉丁字母 $A,B,C,\cdots$(或带有下标的字母 $A_1,B_1,C_1,\cdots$)来命名集合. 特殊的集合,采用特殊的记号.

对于定义 1.2.1 还须补充说明:

(1) 集合中的元素,可以是具体的(直观上可以触摸的,可观测的),也可以是抽象的(想象的).

(2) 集合中的元素是"确定"的,可以明确地区分不同的元素,集合中的元素是"不相同"的("相同"的元素看做是一个).

(3) 元素与集合间的"属于关系"是确定的. 对于某个元素 a 与某个集合 S,要么 $a\in S$,要么 $a\notin S$,二者必居其一,绝无其他情况产生.

(4) 由元素构成的集合,是一个已经"形成"的整体,而不是"正在形成"的整体. 例如,"自然数的全体"是一个集合. 而宇宙中所有的"星体",则不能看做是一个集合.

例 1.2.2 集合的实例

(1) 自然数全体(包括数字"0"在内). ($\mathbf{N}$).

(2) 非零自然数的全体. ($\mathbf{N}^+$).

(3) 整数全体. ($\mathbf{Z}$).

(4) 非负整数的全体. ($\mathbf{Z}^+$).

(5) 有理数全体. ($\mathbf{Q}$).

(6) 实数全体. ($\mathbf{R}$).

(7) 复数全体. ($\mathbf{C}$).

(8) 素数全体. ($\mathbf{P}$).

(9) 小于 10 的素数的集合.

(10) 方程式: $x^2-5x+7=0$ 的所有"实根"的集合.

(11) 两条平行线的"交点"的集合.

(12) 英文字母表.

(13) 鲁迅《狂人日记》中所有的汉字.

(14) Fortran 语言中,所有的标识符构成的集合.

(15) 平面上所有的单位圆周.

1.3 集合及其表示法

集合论中,对于集合有一种系统的表示方法.

1.3.1 显式法(枚举法)

这种方法是把集合中所有的元素统统列(枚)举出来,置于花括号内,例如

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$$

就表示由数字:0, 1, 2, 3, 4, 5, 6, 7, 8, 9 构成的集合. 有时为了节省,也可简记为

$$\{0, 1, 2, 3, \cdots, 9\},$$

其中"…"代表省去了的 4, 5, 6, 7, 8 这 5 个数字. 但是,如果集合中仅含若干个(比如 3 个)互不相干的数字,例如

$$\{1, 8, 17\},$$

就不能缩写为

$$\{1, \cdots, 17\},$$

而必须逐个地写出来.

因此,原则上说,枚举法只适用于表示有限集合.

1.3.2 隐式法

这种方法不要求列出集合中全部元素,只要求给出集合中元素的"特性",即数学中常说的"条件". 例如

$$A = \{x \mid x \text{ 是不大于 } 10^{26} \text{ 的正整数}\},$$

其中竖杠“|”前面的 x 代表集合 A 中的任意元素，竖杠后面所写的一句话代表元素 x 具有的性质（或满足的条件）.

与元素 x 有关的性质，通常简记成 $R(x)$，它表示：“x 有性质 R”. 因此，上述集合 A 可表示为：

$$A = \{x \mid R(x)\}.$$

这种表示集合的方法，称为隐式法.

集合的显式法与隐式法不是互相对立的，为了研究的方便，可以采用不同的表示法. 例如对于同一个集合，可以有不同的表示法：

$$X = \{-3, -2, -1, 0, 1, 2, 3\},$$
$$X = \{x \mid x \in \mathbf{Z}, -3 \leqslant x \leqslant 3\},$$
$$X = \{x \mid x \in \mathbf{Z}, |x| \leqslant 3\}.$$

在隐式法中，确定 $R(x)$ 是关键问题，在计算机科学中，常常要求 $R(x)$ 是一个生成过程.

定义 1.3.1 设 $R(x)$ 是由下述两条规则产生的：

(1) 已知若干初始元素具有性质 R；

(2) $R(x)$ 中其余的元素，均可按某种“构造性”规则产生出来.

则称 $R(x)$ 是集合 $S = \{x \mid R(x)\}$ 的**生成过程**(generating procedure).

例 1.3.2 集合 $M_{2^n} = \{$自然数 2 的幂的全体$\}$.

集合 M_{2^n} 可缩写成

$$M_{2^n} = \{1, 2, 4, 8, 16, \cdots\};$$

也可表示为

$$M_{2^n} = \{m \mid (1) 1 \in M_{2^n}, (2) \text{ 若 } m \in M_{2^n}, \text{ 则 } 2m \in M_{2^n}\}$$

其中生成过程 $R(m)$：(1) $1 \in M_{2^n}$，(2) 若 $m \in M_{2^n}$，则 $2m \in M_{2^n}$.

其中自然数“1”是初始元素，其余的元素 2, 4, 6, 8, 16, … 均可由规则(2)产生出来.

例 1.3.3 集合 $F=\{\text{Fibonacci 数}\}$.

集合 F 可表示如下：

$F=\{F_n \mid (1)\ F_0=F_1=1,\ (2)\ F_{n+1}=F_n+F_{n-1},\ n\in \mathbf{N}^+\}$,
生成过程由(1),(2)给出. F 中的初始元素是 $F_0=1, F_1=1$,其余的元素是

$$
\begin{aligned}
F_2 &= F_1+F_0=2,\\
F_3 &= F_2+F_1=3,\\
F_4 &= F_3+F_2=5,\\
&\cdots\cdots\\
F_{n+1} &= F_n+F_{n-1},\\
&\cdots\cdots
\end{aligned}
$$

1.3.3 特征函数法

这种方法是用一个刻画集合中所有元素的特征函数,来表示集合.

定义 1.3.4 设 A 为集合,若函数 $\mu_A(\cdot)$满足：

$$
\mu_A(x)=\begin{cases}1, & x\in A,\\ 0, & x\notin A.\end{cases}
$$

则称 $\mu_A(\cdot)$为集合 A 的**特征函数**(characteristic function).

由此可知,集合有种种表示法. 通过表格形式表示集合,就是显式法;通过元素的性质来表示集合,就是隐式法. 还可以通过元素对集合的隶属程度的特征函数来表示集合. 通过定义 1.3.4 可知,古典集合的特征函数的值域是一个仅含两个元素的集合 $\{0,1\}$;如果把特征函数的值域拓广为闭区间$[0,1]$(也就是说由有限集合$\{0,1\}$,拓广为无限集合$[0,1]$),则由特征函数确定的集合就是模糊集(fuzzy set).

1.4 子集与集合的包含关系

研究集合时，判断一个集合 A 是否包含在另一个集合 B 中，在理论或实践中都是极其重要的.

定义 1.4.1 设集合 A 与 B，若 A 的每一个元素都是 B 的元素，则称 A 是 B 的**子集**(subset)，记为：

$$A \subseteq B \quad (\text{或 } B \supseteq A),$$

读作：B 包含 A(或 A 包含于 B 中). 称$\subseteq$(或$\supseteq$)为**包含关系**(inclusion relation).

如果 A 不是 B 的子集，记作：

$$A \nsubseteq B.$$

定义 1.4.2 若 A 是 B 的子集，而且集合 B 中至少有一个元素不属于 A，则称 A 是 B 的**真子集**(proper set). 记作

$$A \subset B \quad (\text{或 } B \supset A),$$

称$\subset$(或$\supset$)为**真包含关系**(properly inclusive relation).

必须指出，有些文献中只有符号 $A \subset B$ 而无 $A \subseteq B$，并不严格区分包含关系与真包含关系. 但是，这是两种完全不同的关系，绝对不可混淆.

$A \subseteq B$，$C \nsubseteq D$ 如图 1.1 所示.

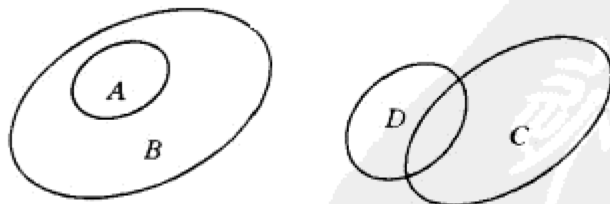


图 1.1

例 1.4.3 下列集合的包含关系与真包含关系是正确的.

$$\mathbf{N} \subset \mathbf{Z},\ \mathbf{Z} \subset \mathbf{Q},\ \mathbf{Q} \subseteq \mathbf{R},\ \mathbf{R} \subseteq \mathbf{C},$$

$$\{0,1\} \subseteq \{0,1\}, \{0,1\} \not\subset \{0,1\}, \{0,1\} \subset [0,1].$$

在包含关系与子集概念的基础上,可以定义集合相等的概念.

定义 1.4.4 设 A,B 是两集合,若 $A \subseteq B$ 且 $B \subseteq A$,则称集合 A 与集合 B **相等**(equal). 记作 $A=B$. 有时简单地记作:

$$A = B \Leftrightarrow A \subseteq B \,\&\, B \subseteq A.$$

注 不要把属于关系与包含关系相混淆,前者表示集合中的元素与集合的一种从属关系(隶属关系),是两个层次之间的关系;而后者则是两个集合之间的关系,是同一个层次之间的关系,它们是两种截然不同的关系.

例 1.4.5

$$\{a\} \not\subset \{\{a\}, b\}, \quad \{a\} \in \{\{a\}, b\},$$
$$\{1,2\} \subset \{0,1,2\}, \quad \{1,2\} \notin \{0,1,2\}.$$

在集合论中,为了研究的方便与理论的系统化,有时需要引入空集的概念.

定义 1.4.6 不含元素的集合,称为**空集**(empty set),记作$\varnothing$.

按照此定义,对于任何集合 A 均有

$$\varnothing \subset A, \ \varnothing \subseteq A, \ \varnothing \subseteq \varnothing.$$

换言之,空集是任何集合的子集(真子集). 此外,还可以证明,空集只有一个. 因此,空集常用特定的记号$\varnothing$标记.

2 集合代数

2.1 集合上的运算

集合上有各种运算，通过各种运算展示出集合间的种种联系，使得集合论有广泛的应用. 首先介绍集合上的基本运算.

2.1.1 集合上的基本运算

最重要的是下述3种：并运算，交运算与差运算. 它们是各种复杂运算的基础.

定义 2.1.1 设 A,B 是两集合，则 $A\cup B$ 为下述集合：

$$A\cup B=\{x\mid x\in A 或 x\in B\},$$

称为 A 与 B 的**并集**(union). 称运算 $\cup$ 是**并运算**. 图 2.1 中阴影部分就是 $A\cup B$.

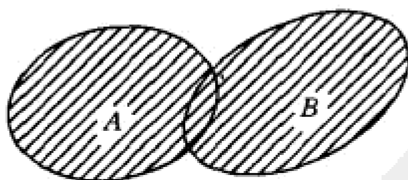


图 2.1

注 不要把“并集”与“并运算”混淆起来，这是两种不同的概念. 并集是一个集合，而并运算是集合上的一种运算. 如同在初等代数中，应严格区分两数之“和”与两数的“加法”运算，两数之“和”仍旧是一个“数”，而“加法”则是作用于“数”上的“运算”.

例 2.1.2 并集与并运算

$$\{1,2,3\} \cup \{3,4,5\} = \{1,2,3,4,5\},$$
$$\{a,b\} \cup \{a\} = \{a,b\},$$
$$\{2,4\} \cup \varnothing = \{2,4\},$$
$$\mathbf{N} \cup \mathbf{N}^{+} = \mathbf{N},$$
$$\mathbf{Q} \cup \mathbf{N} = \mathbf{Q}.$$

注 虽然元素“3”在集合$\{1,2,3\}$及$\{3,4,5\}$中同时出现，但是在并集$\{1,2,3,4,5\}$中只能出现一次(参看定义 2.1.1).

集合的“并运算”，有时也称为“和运算”或“加法”.

集合的并运算可以推广到由多个集合构成的集合族.

定义 2.1.3 设 $A_i(i\in I)$是一族集合，则集合

$$\bigcup_{i\in I} A_i = \{x \mid 有\ i_0 \in I,使得\ x \in A_{i_0}\},$$

称为族 $A_i(i\in I)$的**并**(集).

定义 2.1.4 设 A,B 是两集合，则 $A\cap B$ 为下述集合：

$$A \cap B = \{x \mid x \in A 且 x \in B\},$$

称为 A 与 B 的**交集**(intersection)，称运算 $\cap$ 为**交运算**(intersection operation). 图 2.2 中阴影部分，就是 $A\cap B$.

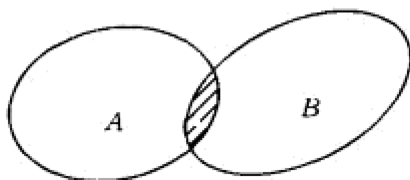


图 2.2

注 不要把“交集”与“交运算”混淆起来，这是不同的概念. 交集是一个集合，而交运算是集合上的一种运算. 如同在初等代数中，应严格区分两数之“积”与两数的“乘法”运算. 两数之“积”仍旧是一个“数”，而“乘法”则是一种“运算”.

集合的“交运算”有时也称为“积运算”或“乘法”.

例 2.1.5 交集与交运算

$$\{1,2,3\} \cap \{2,4,6\} = \{2\},$$
$$\{b_2, b_3, b_4\} \cap \{b_2, b_3, b_4\} = \{b_2, b_3, b_4\},$$
$$\{1,2\} \cap \{3,4\} = \varnothing,$$
$$\{a,b\} \cap \varnothing = \varnothing.$$

由例 2.1.5 可以看出,$A \cap B = \varnothing$ 就相当于集合 A 与 B 不相交. 可见空集概念的引入可以带来叙述上的简练.

集合的交运算也可以推广到集合族.

定义 2.1.6 设 $A_i(i \in I)$ 是一族集合,则集合

$$\bigcap_{i \in I} A_i = \{x \mid \text{对于所有的 } i \in I,\ x \in A_i\},$$

称为族 $A_i(i \in I)$ 的**交**(集).

定义 2.1.7 设 A, B 是两集合,则集合 $A \backslash B$(或 $A - B$)为下述集合:

$$A \backslash B = \{x \mid x \in A \text{ 且 } x \notin B\},$$

称为集合 A 与 B 的**差集**(substraction),称运算"\"("—")是**差运算**(substraction operation). 图 2.3 中的阴影部分,就是 $A \backslash B$.

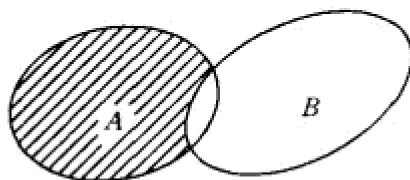


图 2.3

例 2.1.8

$$\{1,2,3\} \backslash \{1,2\} = \{3\},$$
$$\{1,2,3\} \backslash \{1,2,4\} = \{3\},$$
$$\{1,2,3\} \backslash \varnothing = \{1,2,3\},$$
$$\varnothing \backslash \{1,2,3\} = \varnothing,$$
$$\{1,2,3\} \backslash \{1,2,3\} = \varnothing,$$

$$\{1,2,3\}\backslash\{1,2,3,4\}=\varnothing,$$
$$\{1,2,3\}\backslash\{4,5,6\}=\{1,2,3\}.$$

注 由例 2.1.8 可以看出，由 $A\backslash B=A\backslash C$ 得不出 $B=C$ 的结论. $B\backslash A=C\backslash A$ 也得不出 $B=C$ 的结论.

2.1.2 基本运算的重要性质

集合的 3 种基本运算，有下列重要性质，这些性质极为常用，陈述在下列定理中.

定理 2.1.9 设 A,B,C 是集合，则有性质如下：

(1) $A\cup A=A$; （幂等律）
$A\cap A=A$.

(2) $A\cup B=B\cup A$; （交换律）
$A\cap B=B\cap A$.

(3) $A\cup(B\cup C)=(A\cup B)\cup C$; （结合律）
$A\cap(B\cap C)=(A\cap B)\cap C$.

(4) $(A\cup B)\cap A=A$; （吸收律）
$(A\cap B)\cup A=A$.

(5) $A\cup\varnothing=A$. （恒等律）

(6) $A\cap\varnothing=\varnothing$. （零律）

(7) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$; （第一分配律）
$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$. （第二分配律）

(8) $A\backslash A=\varnothing$.

(9) $A\backslash(B\cup C)=(A\backslash B)\cap(A\backslash C)$;
$A\backslash(B\cap C)=(A\backslash B)\cup(A\backslash C)$.

(10) $A\backslash B=A\backslash(A\cap B)$.

(11) $A\backslash(A\backslash B)=A\cap B$.

(12) $(A\backslash B)\backslash C=A\backslash(B\cup C)$;
$(A\backslash B)\backslash C=(A\backslash C)\backslash(B\backslash C)$.

(13) $A\backslash(B\backslash C)=(A\backslash B)\cup(A\cap C)$.

(14) $A\cap(B\backslash C)=(A\cap B)\backslash(A\cap C)$;

$A\cap(B\backslash C)=(A\backslash B)\backslash C$.

定理 2.1.10 设 A,B,C 是集合,则有

(1) $A\cup B\subseteq C\Leftrightarrow A\subseteq C$ 且 $B\subseteq C$.

(2) $A\subseteq B\cap C\Leftrightarrow A\subseteq B$ 且 $A\subseteq C$.

(3) $(A\backslash B)\cup B=A\Leftrightarrow B\subseteq A$.

(4) $(A\cap B)\cup C=A\cap(B\cup C)\Leftrightarrow C\subseteq A$.

(5) $A\subseteq B\Rightarrow A\cup C\subseteq B\cup C$.

(6) $A\subseteq B\Rightarrow A\cap C\subseteq B\cap C$.

(7) $A\subseteq B\Rightarrow(A\backslash C)\subseteq(B\backslash C)$.

(8) $A\subseteq B\Rightarrow(C\backslash B)\subseteq(C\backslash A)$.

(9) $A\cup B=A\cap B\Leftrightarrow A=B$.

定理 2.1.11 设$\{A_k\}$, $\{B_k\}$, $\{A_{kt}\}$, $(k\in K,\ t\in T)$均为集族,则有

(1) $(\bigcup_{k\in K}A_k)\cup(\bigcup_{k\in K}B_k)=\bigcup_{k\in K}(A_k\cup B_k)$.

(2) $\bigcup_{k\in K}\bigcup_{t\in T}A_{kt}=\bigcup_{t\in T}\bigcup_{k\in K}A_{kt}$.

(3) $\bigcap_{k\in K}\bigcap_{t\in T}A_{kt}=\bigcap_{t\in T}\bigcap_{k\in K}A_{kt}$.

(4) $\bigcup_{k\in K}(B\cap A_k)=B\cap(\bigcup_{k\in K}A_k)$.

(5) $\bigcap_{k\in K}(B\cup A_k)=B\cup(\bigcap_{k\in K}A_k)$.

(6) $\bigcup_{k\in K}\bigcap_{t\in T}A_{kt}\subseteq\bigcap_{t\in T}\bigcup_{k\in K}A_{kt}$.

2.1.3 集合的对称差

除了基本运算以外,集合的"对称差"也是一种常见的重要运算,它在数学形态学中频繁地出现."对称差"[①]这种运算,可以用

① "对称差"又称"Minkowski 和".

基本运算定义如下.

定义 2.1.12 设 A,B 是两集合,则集合

$$A \dot{-} B = (A \backslash B) \cup (B \backslash A),$$

称为集合 A 与 B 的**对称差**(symmetric difference). 运算 $\dot{-}$ 称为**对称差运算**(symmetric difference operation). 图 2.4 中的阴影部分,就是 $A \dot{-} B$.

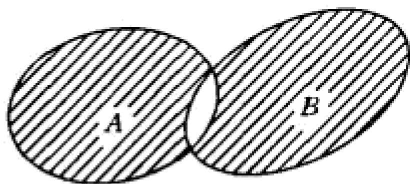


图 2.4

对称差的记号有多种,如 $A \Delta B$, $A \oplus B$, $A \dotplus B$. 关于对称差,有下述重要性质.

定理 2.1.13 设 A,B,C 为集合,则有

(1) $A \dot{-} B = B \dot{-} A$. (交换律)

(2) $A \dot{-} (B \dot{-} C) = (A \dot{-} B) \dot{-} C$. (结合律)

(3) $A \cap (B \dot{-} C) = (A \cap B) \dot{-} (A \cap C)$. (分配律)

(4) $A \dot{-} \varnothing = A$.

(5) $A \dot{-} A = \varnothing$.

(6) $A \dot{-} (A \dot{-} B) = B$.

(7) $A \cup B = A \dot{-} B \dot{-} (A \cap B)$
$= (A \dot{-} B) \cup (A \cap B)$.

(8) $A \backslash B = A \dot{-} (A \cap B)$.

定理 2.1.14 设 $A_1, A_2, \cdots, A_n$, B_1, $\cdots$, B_n 为集合,则有

(1) $(A_1 \cup \cdots \cup A_n) \dot{-} (B_1 \cup \cdots \cup B_n) \subseteq (A_1 \dot{-} B_1) \cup \cdots \cup (A_n \dot{-} B_n)$.

(2) $(A_1 \cap \cdots \cap A_n) \dot{-} (B_1 \cap \cdots \cap B_n) \subseteq (A_1 \dot{-} B_1) \cap \cdots$

$\bigcap (A_n \dot{-} B_n)$.

定理 2.1.15 设 A,B,C 为集合,则有

(1) $A \dot{-} B = \varnothing \Leftrightarrow A = B$.

(2) $A \cap B = \varnothing \Rightarrow A \cup B = A \dot{-} B$.

(3) $A \dot{-} B = C \Leftrightarrow B \dot{-} C = A$,

$$\Leftrightarrow C \dot{-} A = B.$$

2.1.4 幂集与幂运算

由已知集合,通过集合上的运算可以产生新的集合. 反之,也可以对任意复杂的集合进行分解,用较简单的集合通过适当的运算表示出来.

由已知集合产生新集合的诸运算中,还有一种强有力的运算,就是通过选取"子集"的方法来达到的.

设集合 A 如下:

$$A = \{1,2,3\}.$$

考虑 A 的所有子集合. 显然 $\varnothing$ 是它的一个子集,此外 $\{1\}$, $\{2\}$, $\{3\}$, $\{1,2\}$, $\{1,3\}$, $\{2,3\}$, $\{1,2,3\}$ 都是它的子集. 它一共有 2^3 个子集. 以这 8 个子集为元素构成的新集合,称为集合 A 的幂集. 记作:

$$\mathscr{P}(A) = \{\varnothing, \{1\},\{2\},\{3\},\{1,3\},\{1,2\},\{2,3\},\{1,2,3\}\}.$$

定义 2.1.16 设 A 是集合,以 A 的所有子集为元素的集合,称为 A 的**幂集**(power set),记作 $\mathscr{P}(A)$:

$$\mathscr{P}(A) = \{X \mid X \subseteq A\}.$$

运算 $\mathscr{P}(\cdot)$ 称为**幂运算**(power operation).

这种以集合为元素构成的集合,常称为**集族**(family of sets).

一般而言,一个集合 A 的幂集总有

$$\varnothing \in \mathscr{P}(A),$$

$$A \in \mathscr{P}(A).$$

而空集$\varnothing$的幂集 $\mathscr{P}(\varnothing)$就不再是空集，其实

$$\mathscr{P}(\varnothing)=\{\varnothing\}$$

是一个单元素集.

对于幂集 $\mathscr{P}(A)$，还可以产生新的幂集，$\mathscr{P}(\mathscr{P}(A))$，$\mathscr{P}(\mathscr{P}(\mathscr{P}(A)))$，等等.

幂集与幂运算有下列重要性质.

定理 2.1.17 设 $A,B,A_i,B_i,i\in I$ 为集合，则有

(1) $\mathscr{P}(A\cap B)=\mathscr{P}(A)\cap\mathscr{P}(B)$.

(2) $\mathscr{P}(\bigcap_{i\in I}A_i)=\bigcap_{i\in I}\mathscr{P}(A_i)$.

(3) $\mathscr{P}(A\cup B)=\{A_i\cup B_i\mid A_i\in\mathscr{P}(A)$ 且 $B_i\in\mathscr{P}(B)\}$.

(4) $\mathscr{P}(\bigcup_{i\in I}A_i)=\{\bigcup_{i\in I}B_i\mid B_i\in\mathscr{P}(A_i)\}$.

2.2 集合的 Venn 图

在研究集合间的关系时，常常是研究某些同类的集合，即研究某个特定集合 U 的全部子集，这时常称 U 为**全集**(universal).

在研究全集 U 中诸子集时，为了直观，常把 U 设想成二维平面上所有点构成的点集，而 U 的非空子集常表示成平面上由闭曲线所围成的点集(边界点不包括在内)；这些图形统称为 **Venn 图**(纪念英国逻辑学家 John Venn)，如图 2.5.

由于空集$\varnothing$中不含元素，所以不能有 Venn 图，或者可以理解成平面 U 上退化了的图.

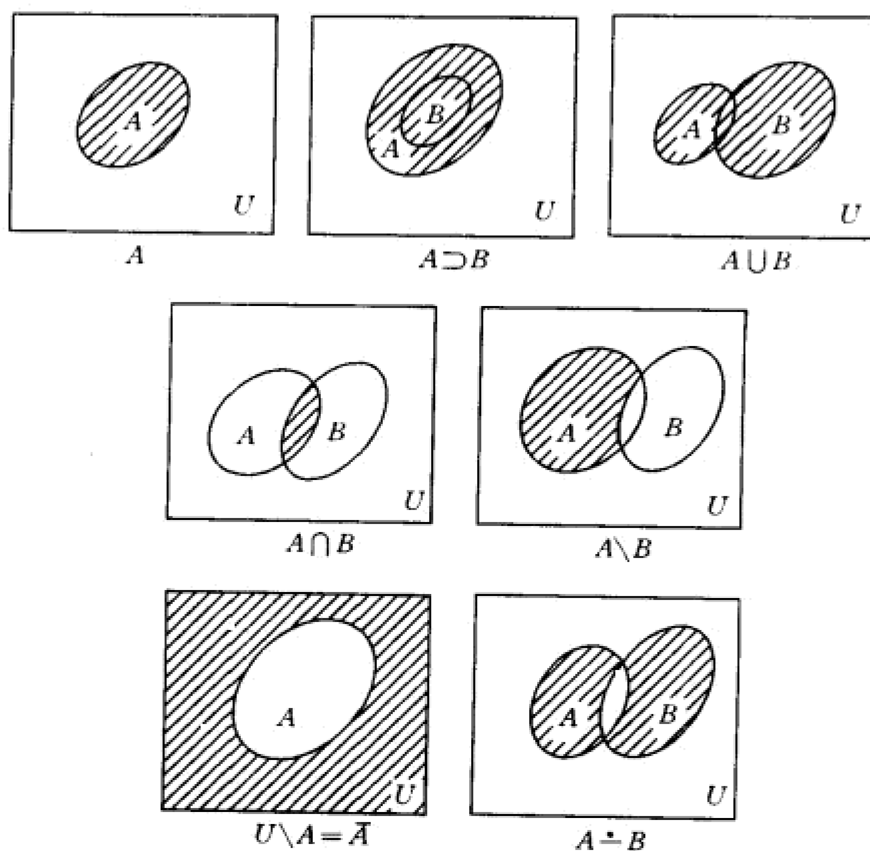
关于全集与补集，有重要性质如下.

定理 2.2.1 设 A,B,C 均为 U 中的子集，则有

(1) $A\cup\varnothing=\varnothing\cup A=A$; (恒等律)

$A\cap\varnothing=\varnothing\cap A=\varnothing$.

(2) $A\cup\overline{A}=A\cup A^c=U$; (互补律)



A　　$A \supset B$　　$A \cup B$

$A \cap B$　　$A \setminus B$

$U \setminus A = \overline{A}$　　$A \dot{-} B$

图 2.5

$A \cap \overline{A} = A \cap A^c = \varnothing$.

(3) $\overline{\overline{A}} = \overline{(\overline{A})} = (A^c)^c = A$. （否定律）

(4) $A \cup U = U \cup A = U$; （零律）

$A \cap \varnothing = \varnothing \cap A = \varnothing$.

(5) $\overline{(A \cup B)} = (A \cup B)^c = \overline{A} \cap \overline{B} = A^c \cap B^c$; （DeMorgan 律）

$\overline{(A \cap B)} = (A \cap B)^c = \overline{A} \cup \overline{B} = A^c \cup B^c$.

(6) $(A \cap B) \cup (A \cap \overline{B}) = (A \cap B) \cup (A \cap B^c) = A$;

$(A \cup B) \cap (A \cup \overline{B}) = (A \cup B) \cap (A \cup B^c) = A$.

(7) $A \cap (\overline{A} \cup B) = A \cap B$;

$A \cap (A^c \cup B) = A \cap B$.

注 补集 $\overline{A}$,有时也记作 A^c.

定理 2.2.2 广义 DeMorgan 律 设 $\{A_k\}, k\in K$ 是 U 中的子集族,则有

(1) $\overline{(\bigcup_{k\in K} A_k)} = \bigcap_{k\in K} \overline{A}_k$.

(2) $\overline{(\bigcap_{k\in K} A_k)} = \bigcup_{k\in K} \overline{A}_k$.

定理 2.2.3 设 A, B, C 都是全集 U 中的子集,则有

(1) $A\subseteq B \Leftrightarrow \overline{A}\cup B=U$.

(2) $A\cap B\subseteq C \Leftrightarrow A\subseteq \overline{B}\cup C$.

(3) $A\subseteq B\cup C \Leftrightarrow A\cap \overline{B}\subseteq C$.

(4) $A\subseteq B \Leftrightarrow \overline{A}\supseteq \overline{B}$.

(5) $A=\overline{B} \Leftrightarrow A\cap B=\varnothing$ 且 $A\cup B=U$.

(6) $\overline{A}=A\dot{-}U$.

(7) $A\backslash B=A\cap \overline{B}$.

注 2.2.4 集合的三种基本运算,$\cup, \cap, \backslash$ 也可以用对称差与交运算或者并运算来定义,也可用差运算与对称差两种运算来定义.

但是可以证明:差运算不能用交运算与并运算来定义;并运算也不能用交运算与差运算来定义.

因此从集合代数的角度看,集合上的基本运算可供选择的是下述情况之一:

(1) $\cup, \cap, \backslash$.

(2) $\cup, \dot{-}$.

(3) $\cap, \dot{-}$.

(4) $\backslash, \dot{-}$.

一般情况下,经常选用的基本运算是 $\cup, \cap, \backslash$.

3 关系

3.1 关系及其表示法

集合中的元素间，通常总有某种关系. 以自然数 N 而言，任意两个自然数总是可以区分"大小"的. 例如，2 与 3 之间，就有一种"大小"关系. 精确地说，就是"小于等于"关系(或"不大于"关系).

$$2 \leqslant 3.$$

在集合论研究中，我们把"关系"这个概念理解成它的外延，并把它看做是一种特殊的集合. 这种集合中的元素是"有序对"(或"有序 n 元组")或是向量. 例如，自然数集 N 上的关系"$\leqslant$"就是集合 R，

$$R = \{\langle x, y\rangle \mid x \in \mathbf{N},\ y \in \mathbf{N},\ x \leqslant y\},$$

因此

$$\langle x, y\rangle \in R \Leftrightarrow x \leqslant y.$$

习惯上，常把 $\langle x, y\rangle \in R$，记作 xRy.

集合 R 中的元素，有下述重要特点：

(1) 若 $x \neq y$，则 $\langle x, y\rangle \neq \langle y, x\rangle$.

(2) 若 $\langle x, y\rangle = \langle u, v\rangle$，则 $x = u$ 且 $y = v$. 反之亦然.

为了一般地研究"关系"，必须先介绍 Descartes 积.

3.1.1 集合的 Descartes 积

定义 3.1.1 设 $A_1, \cdots, A_n$ 为 n 个集合，称集合

$$A_1 \times \cdots \times A_n = \{\langle x_1, \cdots, x_i, \cdots, x_n\rangle \mid x_i \in A_i,\ \forall i \in \mathbf{N}^+\}$$

为由 $A_1,\cdots,A_n$ 构成的 **Descartes 积**.

$A_1\times\cdots\times A_n$ 中的元素 $\langle x_1,\cdots,x_i,\cdots,x_n\rangle$ 称为**有序 n 元组**(n-type),有时也称为**向量**(vector), x_i 称为向量的第 i 个**分量**(component),或**坐标**(coordinate). 特别当 $A_1=A_2=\cdots=A_n=A$ 时,简记 $\underbrace{A\times\cdots\times A}_{n个}$ 为 ${}^nA$.

例 3.1.2 设 $A=\{1,2,3,4\}$, $B=\{c,d\}$, 则 $A\times B=\{\langle 1,c\rangle,\langle 1,d\rangle,\langle 2,c\rangle,\langle 2,d\rangle,\langle 3,c\rangle,\langle 3,d\rangle,\langle 4,c\rangle,\langle 4,d\rangle\}$.

例 3.1.3 二维欧氏平面与三维欧氏空间,分别是 ${}^2\mathbf{R}$ 与 ${}^3\mathbf{R}$.

例 3.1.4 设 $[a,b]$, $[c,d]$ 是由实数构成的区间,则 $[a,b]\times[c,d]$ 是二维欧氏平面上的矩形区域.

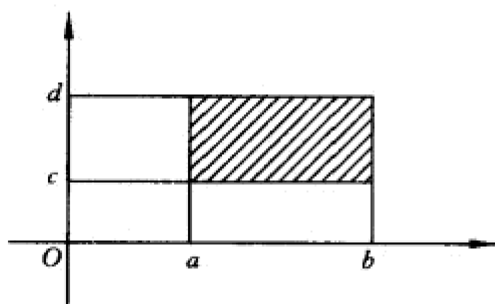


图 3.1

集合的 Descartes 积有下面重要性质.

定理 3.1.5 设 A,B,C,D 为任意集合,则有性质

(1) $A\subseteq B$ 且 $C\subseteq D\Leftrightarrow A\times C\subseteq B\times D$.

(2) $A=B$ 且 $C=D\Leftrightarrow A\times C=B\times D$.

(3) $(A\cap B)\times(C\cap D)=(A\times C)\cap(B\times D)$.

(4) $(A\cup B)\times(C\cup D)\supseteq(A\times C)\cup(B\times D)$.

(5) $A\times(B\cup C)=(A\times B)\cup(A\times C)$.

(6) $(A\cup B)\times(C\cup D)=(A\times C)\cup(B\times C)\cup(A\times D)\cup$

$(B\times D)$.

(7) $(A\backslash B)\times C=(A\times C)\backslash(B\times C)$.

(8) $A\times(B\backslash C)=(A\times B)\backslash(A\times C)$.

定理 3.1.6 设 A_i,B_i,A_k,B_t 为任意集合,则有性质

(1) $(\bigcap_{i\in I}A_i)\times(\bigcap_{i\in I}B_i)=\bigcap_{i\in I}(A_i\times B_i)$.

(2) $(\bigcup_{k\in K}A_k)\times(\bigcup_{t\in T}B_t)=\bigcup_{(k,t)\in K\times T}(A_k\times B_t)$.

(3) $(\bigcap_{k\in K}A_k)\times(\bigcap_{t\in T}B_t)=\bigcap_{(k,t)\in K\times T}(A_k\times B_t)$.

注 3.1.7 一般而言,对于集合的 Descartes 积,交换律与结合律不恒成立.

$$A\times B\neq B\times A,$$
$$(A\times B)\times C\neq A\times(B\times C).$$

为使用方便,约定

$$A\times\varnothing=\varnothing\times A=\varnothing.$$

3.1.2 *n* 元关系

建立集合的 Descartes 积的概念之后,可以定义 n 元关系.

定义 3.1.8 设 $A_1,\cdots,A_n$ 为 n 个集合,集合 $A_1\times\cdots\times A_n$ 中的子集 R 为

$$R\subseteq A_1\times\cdots\times A_n,$$

称为以 $A_1,\cdots,A_n$ 为基的 ***n* 元关系**(n-relation).

当 $R\subseteq{}^2A=A\times A$ 时,称 R 是集合 A 上的**二元关系**(binary relation).

当 $R\subseteq A$ 时,称 R 是集合 A 上的**一元关系**(unary relation).实际上,R 是 A 的子集.

当 $R=\varnothing$ 时,称为**空关系**(empty relation).

当 $R=A_1\times\cdots\times A_n$ 时,称为**全关系**(total relation).

例 3.1.9 三维欧氏空间中,半径为 a 的球面是 ${}^3\mathbf{R}$ 上的三元

关系.

设 S 是 ${}^3\mathbf{R}$ 中的球面,则

$$S=\{\langle x,y,z\rangle\in{}^3\mathbf{R}\mid\langle x_0,y_0,z_0\rangle\in{}^3\mathbf{R},(x-x_0)^2+(y-y_0)^2+(z-z_0)^2=a^2\}.$$

例 3.1.10 在关系数据库中,用表格方式表示的文件,也是一种关系 R. 见表 3.1.

表 3.1

部门	姓名	性别	部门电话
水产部	史文心	男	2786
石油部	罗林	男	2482
工业部	卢依人	女	3133
石油部	秦如	女	2482
石油部	李英	男	2482
石油部	王义	男	2482
电力部	王小英	女	3025

表中,$R\subseteq A_1\times A_2\times A_3\times A_4$,

$A_1=\{$水产部,石油部,工业部,电力部$\}$.

$A_2=\{$史文心,罗林,卢依人,秦如,李英,王义,王小英$\}$.

$A_3=\{$男,女$\}$.

$A_4=\{2786,2482,3133,3025\}$.

表格中的每一行,例如

〈石油部,罗林,男,2482〉,

都是 R 中的一个元素.

上述文件 R(表 3.1)就是四维空间 $A_1\times A_2\times A_3\times A_4$,中的一个子集.

3.2 二元关系与映射

本节主要研究最重要的二元关系，以及一种特殊的二元关系——映射.

3.2.1 二元关系

在关系理论中，二元关系占据中心地位，无论在理论上或实践中极为重要. 其原因在于使用上的频繁，以及许多有关多元关系的问题均可归约为二元关系. 此外，它与传统数学中的多值函数有密切的联系.

定义 3.2.1 设 A,B 为集合，$R\subseteq A\times B$，则称 R 是以 A，B 为基的**二元关系**(binary relation). 当 $\langle a,b\rangle\in R$ 时，称 a,b 满足关系 R，记作 aRb.

特别当 $R\subseteq A\times A$ 时，则称 R 是集合 A 上的二元关系.

例 3.2.2 设 $A=\{1,2,3,4\}$，$B=\{5,6\}$. 定义以 A,B 为基的二元关系 R 如下：

$$\langle a,b\rangle \in R \Leftrightarrow a \leqslant b.$$

于是

$$R=\{\langle 1,5\rangle,\langle 1,6\rangle,\langle 2,5\rangle,\langle 2,6\rangle,\\ \langle 3,5\rangle,\langle 3,6\rangle,\langle 4,5\rangle,\langle 4,6\rangle\}.$$

这种关系称为"不大于"关系(或"小于等于"关系).

注 数学中的关系$\leqslant$，在许多场合频繁出现. 因此，在有些文献中，就将关系符号 R 以符号$\leqslant$代替. 这时$\leqslant$的含义不局限于"不大于"关系. 也可记作：

$$\langle a,b\rangle \in \leqslant \Leftrightarrow a \leqslant b.$$

例 3.2.3 设 $A=\{0,1,2,3,4,5,6,7\}$，在 A 上定义二元关系 $R\subseteq {}^2A$ 如下：

$\langle x,y\rangle \in R \Leftrightarrow 2 \mid (x-y)$，(即$(x-y)$可以被 2 整除)，于是

$$
\begin{aligned}
R=\{&\langle 0,0\rangle,\langle 0,2\rangle,\langle 0,4\rangle,\langle 0,6\rangle,\langle 1,1\rangle,\\
&\langle 1,3\rangle,\langle 1,5\rangle,\langle 1,7\rangle,\langle 2,0\rangle,\langle 2,2\rangle,\\
&\langle 2,4\rangle,\langle 2,6\rangle,\langle 3,1\rangle,\langle 3,3\rangle,\langle 3,5\rangle,\\
&\langle 3,7\rangle,\langle 4,0\rangle,\langle 4,2\rangle,\langle 4,4\rangle,\langle 4,6\rangle,\\
&\langle 5,1\rangle,\langle 5,3\rangle,\langle 5,5\rangle,\langle 5,7\rangle,\langle 6,0\rangle,\\
&\langle 6,2\rangle,\langle 6,4\rangle,\langle 6,6\rangle,\langle 7,1\rangle,\langle 7,3\rangle,\\
&\langle 7,5\rangle,\langle 7,7\rangle\}.
\end{aligned}
$$

关系 R 也可用隐式法表示如下：

$$R=\{\langle x,y\rangle \mid 2 \mid (x-y) \text{ 且 } x\in A,\ y\in A\}.$$

这种关系常称为“模 2 同余关系”，在数论中常记作：

$$\langle x,y\rangle \in R \Leftrightarrow x\equiv y \pmod 2.$$

在计算机上，输出定长字符(如字符的长度为 32 位)时，输出打印的“操作”就是“以 32 为模的同余关系”.

例 3.2.4 设 $\mathbf{R}\times\mathbf{R}$ 上的关系 R 定义如下：

$$R=\{\langle x,y\rangle \mid x^2+y^2=1, x\in\mathbf{R},\ y\in\mathbf{R}\}.$$

这个关系是一个以原点为圆心，半径为 1 单位的圆周上全部点所构成的集合.

例 3.2.5 集合 A 的子集之间的包含关系“$\subseteq$”是集合 $\mathscr{P}(A)\times\mathscr{P}(A)$上元素间的二元关系. 即，对于任意的集合 A_1，A_2 满足

$$\langle A_1,A_2\rangle \in\subseteq \Leftrightarrow A_1\subseteq A_2.$$

注 由例 3.2.5 可以看出，一个集合 A 的子集间的包含关系，不是其元素间的二元关系. 这种关系亦可归约为 A 的幂集 $\mathscr{P}(A)$上元素之间的二元关系. 而且这种“提升”的方法，是普遍适用的. 它反映了二元关系的重要性.

例 3.2.6 集合 A 与其元素 a 间的“属于关系”($a\in A$)也是集合 $A\times\mathscr{P}(A)$上的二元关系.

例 3.2.7 数理经济学中，定义于消费集上的“偏好”关系，是

一种二元关系.

对于二元关系，习惯上还有定义域与值域的概念.

定义 3.2.8 设 $R\subseteq X\times Y$ 是二元关系，下述集合

$\mathrm{dom}R=\{x\mid x\in X$, 存在 $y\in Y$ 使得 $\langle x,y\rangle\in R\}$,

$\mathrm{ran}R=\{y\mid y\in Y$, 存在 $x\in X$ 使得 $\langle x,y\rangle\in R\}$,

称 $\mathrm{dom}R$ 是 R 的**定义域**(domain)，$\mathrm{ran}R$ 是 R 的**值域**(range).

3.2.2 关系运算

关系是一种特殊的集合(其中的元素称为向量)，因此凡作用于集合上的运算：$\cup$，$\cap$，$-$，$\setminus$，$\dot{-}$均可作用于关系(集合)上；此外二元关系还有一些特殊的运算. 主要有：逆运算，复合运算以及由复合运算所诱导出的幂运算及闭包运算. 下面研究这些运算的规律.

定义 3.2.9 设 $R\subseteq A\times B$ 是从 A 到 B 的二元关系，则从 B 到 A 的二元关系：

$$R^{-1}=\{\langle y,x\rangle\mid\langle x,y\rangle\in R\}$$

称为 R 的**逆关系**(inverse relation). 运算"$^{-1}$"称为**逆运算**(inverse operation).

逆关系也是一种集合，如果 R 是一个关系，那么 R^{-1} 与 $\bar{R}$(R 的补集)也都是关系，但这是两种不同的关系. 见例 3.2.10.

例 3.2.10 实数集 **R** 上的"<"关系("小于"关系)，它的逆关系是">"关系("大于"关系). 而"<"关系的补关系是"≥"关系("不小于"关系).

例 3.2.11 实数集 **R** 上的"≠"关系("不等"关系)，它的逆关系仍然是"≠"关系("不等"关系)，而它的补关系则是"="关系("相等"关系).

例 3.2.12 整数集 **Z** 上的"整除"关系，它的逆关系则是"倍数"关系.

例 3.2.13 设集合 $A=\{1,2,3\}$, $B=\{a,b,c\}$, $R\subseteq A\times B$ 定义如下

$$R=\{\langle 1,a\rangle,\langle 2,b\rangle,\langle 3,c\rangle\}.$$

它的逆关系

$$R^{-1}=\{\langle a,1\rangle,\langle b,2\rangle,\langle c,3\rangle\}.$$

它的补关系

$$\overline{R}=\{\langle 1,b\rangle,\langle 1,c\rangle,\langle 2,a\rangle,\langle 2,c\rangle,\langle 3,a\rangle,\langle 3,b\rangle\}.$$

定义 3.2.14 设关系 $R\subseteq X\times Y$ 及 $S\subseteq Y\times Z$, 集合 $R\circ S$ 为

$R\circ S=\{\langle x,z\rangle \mid x\in X,\ z\in Z$, 存在 $y\in Y$ 使得 $\langle x,y\rangle\in R$ 且 $\langle y,z\rangle\in S\}$,

称为 R 与 S 的**复合(关系)**(composite), 运算"$\circ$"称为**复合运算**(composite operation).

复合关系如图 3.2 所示.

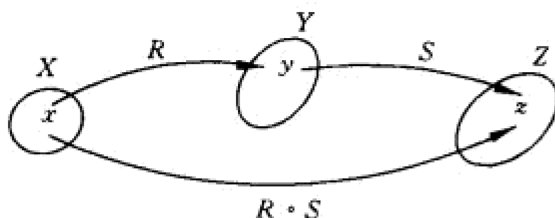


图 3.2

对于复合运算,一般情形 $R\circ S\neq S\circ R$.

例 3.2.15 设关系 $R\subseteq \mathbf{N}\times\mathbf{N}$, $S\subseteq\mathbf{N}\times\mathbf{N}$:

$$R=\{\langle 1,2\rangle,\langle 2,3\rangle,\langle 3,4\rangle\},$$
$$S=\{\langle 4,3\rangle,\langle 2,1\rangle,\langle 1,3\rangle\},$$

则

$$R\circ S=\{\langle 1,1\rangle,\langle 3,3\rangle\},$$
$$S\circ R=\{\langle 4,4\rangle,\langle 2,2\rangle,\langle 1,4\rangle\}.$$

定义 3.2.16 设 R 是集合 A 上的二元关系，则关系 R 的 n 次幂（n-power）R^n 为下述集合：

(1) $R^0=I_A$，($R^0=\{\langle x,y\rangle \mid x\in A,\ y\in A,\ x=y\}$.

(2) $R^{n+1}=R^n\circ R$，$n\in \mathbf{N}$.

以下定理给出关系与各种运算之间的重要性质.

定理 3.2.17 设 R,S,T 都是从集合 A 到集合 B 的二元关系，则有

(1) $R\cup R=R$.

(2) $R\cap R=R$.

(3) $(R^{-1})^{-1}=R$. （幂等性）

(4) $\overline{\overline{R}}=\overline{(\overline{R})}=R$. （幂等性）

(5) $(R\cup S)^{-1}=R^{-1}\cup S^{-1}$. （分配性）

(6) $(R\cap S)^{-1}=R^{-1}\cap S^{-1}$. （分配性）

(7) $(\overline{R})^{-1}=\overline{(R^{-1})}$. （可换性）

(8) $(R\backslash S)^{-1}=R^{-1}\backslash S^{-1}$. （分配性）

(9) $\varnothing^{-1}=\varnothing$. （对称性）

(10) $(A\times B)^{-1}=B\times A$.

(11) $R\supseteq S\Leftrightarrow R^{-1}\supseteq S^{-1}$. （单调性）

(12) $R\supseteq S\Leftrightarrow \overline{R}\subseteq \overline{S}$. （逆单调性）

定理 3.2.18 设 R,S,T 分别是 A 到 B，B 到 C，C 到 D 的二元关系，任意的 $m,n\in \mathbf{N}$，则有

(1) $(R\circ S)\circ T=R\circ (S\circ T)$. （结合律）

(2) $(R\circ S)^{-1}=S^{-1}\circ R^{-1}$.

(3) $R^m\circ R^n=R^{m+n}$. （指数律）

(4) $(R^m)^n=R^{m\times n}$. （指数律）

定理 3.2.19 设 R,S 是 B 到 C 的二元关系，T 是 A 到 B 的二元关系，Q 是 C 到 D 的二元关系，则有

(1) $T\circ (R\cup S)=(T\circ R)\cup (T\circ S)$. （分配律）

(2) $T\circ(R\cap S)\subseteq(T\circ R)\cap(T\circ S)$. （弱分配律）

(3) $R\subseteq S\Leftrightarrow T\circ R\subseteq T\circ S$. （单调性）

(4) $R\subseteq S\Leftrightarrow R\circ Q\subseteq S\circ Q$. （单调性）

定理 3.2.20 设 R,S 是 A 到 B 的二元关系，T 是 B 到 C 的二元关系，则有

(1) $(R\cup S)\circ T=(R\circ T)\cup(S\circ T)$. （分配律）

(2) $(R\cap S)\circ T\subseteq(R\circ T)\cap(S\circ T)$. （弱分配律）

定理 3.2.21 设 X 是有限集，$|X|=n$，R 是 X 上的二元关系，则有

$$\bigcup_{i=1}^{\infty} R^i=\bigcup_{i=1}^{n} R^i.$$

例 3.2.22 设 $\Sigma=\{a,b,\cdots,x,y,z\}$（即英文字母表），

$$R=\{\langle a,b\rangle,\langle b,c\rangle,\langle c,d\rangle,\langle e,f\rangle\}\subseteq\Sigma\times\Sigma,$$

则有

$$\begin{aligned}
R^0&=I_\Sigma=\{\langle a,a\rangle,\langle b,b\rangle,\cdots,\langle x,x\rangle,\\
&\qquad\langle y,y\rangle,\langle z,z\rangle\},\\
R^1&=R,\\
R^2&=R\circ R=\{\langle a,c\rangle,\langle b,d\rangle\},\\
R^3&=R^2\circ R=\{\langle a,d\rangle\},\\
R^4&=R^3\circ R=\varnothing,\\
R^n&=\varnothing\quad(n\geqslant 4).
\end{aligned}$$

例 3.2.23 设 $\Sigma=\{a,b,c,\cdots,x,y,z\}$，$R=\{\langle a,b\rangle,\langle b,c\rangle,\langle c,a\rangle\}\subseteq\Sigma\times\Sigma$，

则有

$$\begin{aligned}
R^0&=I_\Sigma,\\
R^1&=R,\\
R^2&=\{\langle a,c\rangle,\langle b,a\rangle,\langle c,b\rangle\},\\
R^3&=R^2\circ R=\{\langle a,a\rangle,\langle b,b\rangle,\langle c,c\rangle\}=R^0=I_\Sigma,
\end{aligned}$$

$$R^4 = R^3 \circ R = R,$$
$$R^5 = R^4 \circ R = R \circ R = R^2,$$
$$R^6 = R^5 \circ R = R^2 \circ R = R^3 = I_\Sigma,$$
$$R^7 = R^6 \circ R = R^3 \circ R = R,$$
$$\cdots\cdots$$

一般有

$$R^{3+k} \subseteq \bigcup_{i=1}^{3} R^i \qquad (k = 1,2,3,\cdots).$$

当$|R| = n$时,有

$$R^{n+k} \subseteq \bigcup_{i=1}^{n} R^i \qquad (k = 1,2,\cdots).$$

由例 3.2.22,例 3.2.23 可以看出,对于复合运算,经常有

$$\mathrm{dom}(R \circ S) \subseteq \mathrm{dom}R \quad 及 \quad \mathrm{ran}(R \circ S) \subseteq \mathrm{ran}S.$$

因此R^n的基数$|R^n|$总是非增的,当R是有限集合X上的二元关系时,还有定理 3.2.21. 例 3.2.22 与例 3.2.23 是定理 3.2.21 的具体实例.

3.3 特殊的二元关系

3.3.1 概念

本节将集中介绍若干特殊的二元关系,它们在理论上与应用中经常出现.

定义 3.3.1 设R是A上的二元关系.

(1) 若对任意的$x \in A$,满足xRx,则称R是**自反的**(reflexive).

(2) 若对任意的$x \in A$,满足$x \not R x$,则称R是**反自反的**(antireflexive).

(3) 若对任意的$x, y \in A$,满足

$$xRy \Rightarrow yRx,$$

则称 R 是**对称的**(symmetric).

(4) 若对任意的 $x,y \in A$，满足

$$xRy \text{ 且 } yRx \Rightarrow x = y,$$

则称 R 是**反对称的**(antisymmetric).

(5) 若对任意的 $x,y \in A$，满足

$$xRy \Rightarrow y \not R x,$$

则称 R 是**不对称的(非对称的)**(asymmetric).

(6) 若对任意的 $x,y \in A$,满足

$$xRy \text{ 且 } yRz \Rightarrow xRz,$$

则称 R 是**传递的**(transitive).

(7) 若对任意的 $x,y \in A$，满足

$$xRy \text{ 或 } yRx \text{ 或 } x = y,$$

则称 R 是**连接的**(connective).

读者注意,有些文献中,把反对称叫做**弱反对称**(weakly antisymmetric);把不对称(非对称)叫做**反对称或斜对称**.

看下面的实例.

例 3.3.2 任意集合 A 上的恒等关系 I_A 如下：

$$I_A = \{\langle x,x \rangle \mid x \in A\},$$

它是自反,对称,传递关系. 也是反对称的,但不是非对称的.

例 3.3.3 实数集合 $\mathbf{R}$ 上的"不大于关系"($\leqslant$)是自反,反对称,传递关系. 它不是对称关系.

例 3.3.4 实数集合 $\mathbf{R}$ 上的"小于"关系($<$)是反自反的,传递的,同时也是不对称的.

例 3.3.5 设集合 $A=\{1,2,3\}$,R 是 A 上的二元关系：

$$R = \{\langle 2,2 \rangle, \langle 2,3 \rangle, \langle 1,3 \rangle, \langle 3,2 \rangle\},$$

说明 R 的性质.

解 因为 $\langle 1,1 \rangle \notin R$, $\langle 3,3 \rangle \notin R$,所以 R 不是自反的. 但是

$\langle 2,2\rangle \in R$，所以 R 也不是反自反的．由于 $\langle 1,3\rangle \in R$，而 $\langle 3,1\rangle \notin R$，所以 R 不是对称的．由于 $\langle 1,3\rangle \in R$，$\langle 3,2\rangle \in R$ 而 $\langle 1,2\rangle \notin R$，所以 R 不是传递的．由于 $\langle 3,2\rangle \in R$ 且 $\langle 2,3\rangle \in R$，所以 R 也不是非对称的．

从例 3.3.5 可以看出，一个关系不是自反的，并不就是反自反的．不是对称的，并不就是反对称的，也不就是不对称的．

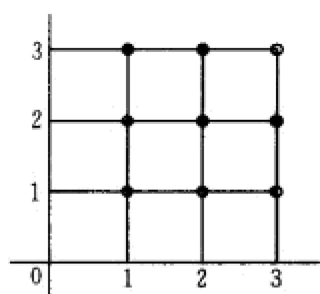


图 3.3

例 3.3.5 中的关系 R 如图 3.3 所示．图中的 9 个圆点（包括"白"点与"黑"点）是集合 $A\times A$，而 $R=\{$"黑"点$\}$（由 4 个"黑"点组成．从"黑"点的几何位置可以直观地看出，由于 R 不包含点 $\langle 1,1\rangle$，$\langle 3,3\rangle$，所以 R 不是自反的，可见自反性是"全局性"的，同样对称性也是"全局性"的，因此 R 也不是对称的．同样可以看出非对称性也是"全局性"的．所以可以说 R 是"局部"自反的，"局部"对称的与"局部"非对称的．

例 3.3.6 设 R 是实数域 $\mathbf{R}$ 上的二元关系，试阐明 R 各种特性的几何解释．

(1) R 是自反的．集合 R 包含二维平面 $\mathbf{R}\times\mathbf{R}$ 中第 1,3 象限的平分角线 $I_{\mathbf{R}}$．

(2) R 是对称的．集合 R 以二维平面 $\mathbf{R}\times\mathbf{R}$ 中第 1,3 象限的平分角线 $I_{\mathbf{R}}$ 为对称轴．

(3) R 是连接的．$R\cup R^{-1}\cup I_{\mathbf{R}}=\mathbf{R}\times\mathbf{R}$．

(4) R 是反自反的．$R\cap I_{\mathbf{R}}=\varnothing$．

(5) R 是不对称的（非对称的）．集合 R 不包含关于 $I_{\mathbf{R}}$ 的对称点．

(6) R 是反对称的．集合 R 关于 $I_{\mathbf{R}}$ 的对称点必在 $I_{\mathbf{R}}$ 上．

例 3.3.6 给出了各种特殊关系的几何解释，读者可以此为背

景深入地理解各种特殊关系的性质.

例 3.3.7 任意集合 A 上的空关系(空集),是自反的,同时又是反自反的.

必须注意,除空关系外,任何非空集合 A 上的任何关系,不能既是自反的又是反自反的. 既是对称的,又是不对称的. 但是任意集合 A 上的恒等关系 I_A 既是对称的又是反对称的.

下面的定理精确地表达了各种特性.

定理 3.3.8 设 R 是集合 A 上的二元关系,则有

(1) R 是自反的 $\Leftrightarrow I_A \subseteq R$.

(2) R 是对称的 $\Leftrightarrow R = R^{-1}$.

(3) R 是传递的 $\Leftrightarrow R \circ R = R$.

(4) R 是反自反的 $\Leftrightarrow R \cap I_A = \varnothing$.

(5) R 是反对称的 $\Leftrightarrow R \cap R^{-1} \subseteq I_A$.

(6) R 是反对称的 $\Leftrightarrow R \setminus I_A$ 是不对称的.

(7) R 是连接的 $\Leftrightarrow R \cup R^{-1} \cup I_A = A \times A$(全关系).

各种关系通过各种运算又可以产生各种新的关系. 比如两个对称关系通过"并"运算产生的并集仍然是一个对称关系. 但是两个传递关系经过"并"运算产生的并集不一定是传递关系. 因此,各种关系在各种运算下,能否保持它原有特性,即对运算的**保持性**问题是一个重要的问题. 为此,有下面的定理.

定理 3.3.9 设二元关系 R,S.

(1) 若 R,S 是自反的,则 $R^{-1}, R\cup S,\ R\cap S,\ R\circ S$ 也是自反的.

(2) 若 R,S 是反自反的,则 $R^{-1},\ R\cup S,\ R\cap S$ 也是反自反的.

(3) 若 R,S 是传递的,则 $R^{-1},\ R\cap S$ 也是传递的.

(4) 若 R,S 是对称的,则 $R^{-1},\ R\cup S,\ R\cap S$ 也是对称的.

(5) 若 R,S 是反对称的,则 $R^{-1},\ R\cap S$ 也是反对称的.

(6) 若 R,S 是非对称的,则 R^{-1}, $R\cap S$ 也是非对称的.

(7) 若 R,S 是连接的,则 R^{-1}, $R\cup S$, $R\cap S$ 也是连接的.

从定理 3.3.9 可见,逆运算,交运算有很好的保持性. 而并运算及复合运算的保持性较差. 许多具有各种特性的关系,经过这些运算后,会丧失原有的特性.

例 3.3.10 设 $A=\{a,b,c,d\}$,二元关系 R,S 如下:

$$R=\{\langle a,b\rangle,\langle b,c\rangle,\langle a,c\rangle\},$$
$$S=\{\langle b,c\rangle,\langle c,d\rangle,\langle b,d\rangle\},$$

则

$$R^{-1}=\{\langle b,a\rangle,\langle c,b\rangle,\langle c,a\rangle\},$$
$$S^{-1}=\{\langle c,b\rangle,\langle d,c\rangle,\langle d,b\rangle\},$$
$$R\cap S=\{\langle b,c\rangle\},$$
$$R\cup S=\{\langle a,b\rangle,\langle b,c\rangle,\langle a,c\rangle,\langle c,d\rangle,\langle b,d\rangle\},$$
$$R\circ S=\{\langle a,c\rangle,\langle b,d\rangle,\langle a,d\rangle\}.$$

其中,R,S 是传递的,而 R^{-1},S^{-1} 也是传递的,但 $R\cup S$ 不是传递的.

3.3.2 关系的限制与扩充

为了获得人们所希望的关系,有时必须在已给的关系(集)中删去一些元素,或者添加适量的元素,从而导致对原有关系的限制与扩充.

定义 3.3.11 设 R 是 A 上的二元关系,B 是 A 中的子集 $B\subseteq A$,称关系 $R\cap(B\times B)$ 是 R 在集合 B 上的**限制**(restriction),记作 $R\upharpoonright B$.

由定义可知 $R\upharpoonright B\subseteq R$. 因此 $R\upharpoonright B$ 是 R 的**子关系**(subrelation).

例 3.3.12 设 $A=\{a,b,c,d\}$,$B=\{a,b\}$, $R\subseteq A\times A$ 如下:

$$R=\{\langle a,a\rangle,\langle b,b\rangle,\langle a,b\rangle,\langle b,a\rangle,\langle b,c\rangle\},$$

$$R \upharpoonright B = \{\langle a,a\rangle,\langle b,b\rangle,\langle a,b\rangle,\langle b,a\rangle\}.$$

显然,关系 R 不是自反的,不是对称的,也不是传递的. 但是 $R \upharpoonright B$ 却同时具有自反、对称、传递的性质.

从广义的角度上看,限制也是作用于集合上的一种“运算”. 如果原有的关系 R 过于庞大而性质欠佳,就可以通过限制运算,选取其中性质优良的子关系.

定义 3.3.13 设 R,S 是 A 上的二元关系,$R \subseteq S$, $S \subseteq A \times A$, 则称 S 是关系 R 的**扩充**(extension),记作 $\mathrm{Ext}R$.

与“限制”一样,“扩充”也是作用于集合上的一种“运算”.

读者注意,一般情形,设 R 是 A 上的关系,显然有 $R \subseteq \mathrm{Ext}R$(这是由于 $R \subseteq A \times A = \mathrm{Ext}R$). 但是如果要求 $\mathrm{Ext}R$ 还具有某种特性(R 所未具有的特性),而又不希望 $\mathrm{Ext}R = A \times A$,这时具有某种特性的扩充是否存在,是一个必须考虑的问题. 看下面的例子.

例 3.3.14 设 $R \subseteq A \times A$ 是二元关系,则必存在自反关系 $\mathrm{Ext}R$.

事实上

$$\mathrm{Ext}R = R \cup I_A.$$

例 3.3.15 设 $R \subseteq A \times A$, $A = \{a,b\}$,其中

$$R = \{\langle a,a\rangle, \langle a,b\rangle\},$$

问是否存在反自反关系 $\mathrm{Ext}R$.

事实上,由于有 $R \subseteq \mathrm{Ext}R$,而 $\langle a,a\rangle \in R$, 从而 $\langle a,a\rangle \in \mathrm{Ext}R$. 所以 R 的任意扩充 $\mathrm{Ext}R$,绝不会是反自反的,即关系 R 的反自反扩充是不存在的.

3.3.3 关系的闭包与闭包运算

本节介绍如何由给定的关系 R 出发构造新的关系 $\mathrm{Ext}R$,使得 $\mathrm{Ext}R$ 具有预定的特性.

定义 3.3.16 设 $R \subseteq A \times A$ 是 A 上的二元关系，若存在最小的自反（对称、传递）关系 $\text{Ext}^* R$，则称它是 R 的**自反（对称、传递）闭包**(closure)，分别记作 $r(R)$，$s(R)$，$t(R)$.

注 (1) 定义 3.3.16 中"最小"的意思是指集合包含意义上的，即对 R 的任意扩充 $\text{Ext}R$，满足

$$\text{Ext}R \supseteq \text{Ext}^* R.$$

(2) 定义 3.3.16 中，没有断定对二元关系 R，这些闭包是否存在；换言之，没有对闭包的存在性作出保证.

关于闭包的存在性及其构造问题，见下述定理.

定理 3.3.17 设 R 是集合 A 上的二元关系，则 R 的自反、对称、传递闭包均存在，且

(1) R 是自反的 $\Leftrightarrow r(R)=R$.

(2) R 是对称的 $\Leftrightarrow s(R)=R$.

(3) R 是传递的 $\Leftrightarrow t(R)=R$.

定理 3.3.18 设 R 是集合 A 上的二元关系，I_A 是 A 上的恒等关系，则

(1) $r(R)=R \cup I_A$.

(2) $s(R)=R \cup R^{-1}$.

(3) $t(R)=\bigcup\limits_{i=1}^{\infty} R^i \quad (=R^1 \cup R^2 \cup \cdots)$.

定理 3.3.18 指出自反、对称和传递闭包是如何构造的.

例 3.3.19 自然数集 **N** 上的"小于"关系($<$)，它的自反闭包 $r(<)$ 是"$\leqslant$"关系. **N** 上的"不相等"关系($\neq$)的自反闭包 $r(\neq)$ 是 **N** 上的全关系 $\mathbf{N} \times \mathbf{N}$. **N** 上空关系 $\varnothing$ 的自反闭包 $r(\varnothing)=I_{\mathbf{N}}$.

例 3.3.20 设二元关系 $R \subseteq \mathbf{N} \times \mathbf{N}$ 如下：

$$R=\{\langle 0,1\rangle,\langle 1,2\rangle,\cdots,\langle n,n+1\rangle,\cdots\},$$

求 $t(R)$.

解

$$R^2 = R \circ R = \{\langle 0,2\rangle, \langle 1,3\rangle, \cdots, \langle n,n+2\rangle, \cdots\},$$
$$R^3 = R^2 \circ R = \{\langle 0,3\rangle, \langle 1,4\rangle, \cdots, \langle n,n+3\rangle, \cdots\},$$
…………………………………………
$$R^i = R^{i-1} \circ R = \{\langle 0,i\rangle, \langle 1,i+1\rangle, \cdots, \langle n,n+i\rangle, \cdots\},$$
…………………………………………

所以

$$t(R) = \bigcup_{i=1}^{\infty} R^i.$$

例 3.3.21 设 $A=\{a,b,c\}$，二元关系 $R \subseteq A \times A$，

$$R = \{\langle a,b\rangle, \langle b,a\rangle, \langle b,c\rangle\}.$$

求 $t(R)$.

解 由于

$$R^2 = R \circ R = \{\langle a,a\rangle, \langle b,b\rangle, \langle a,c\rangle\},$$
$$R^3 = R^2 \circ R = \{\langle a,b\rangle, \langle b,a\rangle, \langle b,c\rangle\} = R,$$
$$R^4 = R^3 \circ R = R \circ R = R^2,$$

于是

$$t(R) = R \cup R^2.$$

定理 3.3.22 设 R 是有限集 A 上的二元关系，则有

$$t(R) = \bigcup_{i=1}^{|A|} R^i.$$

由定理 3.3.22 可知，当 A 为有限集时，关系 R 的传递闭包并非由无穷项构成，关系 R^j 的指数是有限的，当 $j > |A|$ 时，

$$R^j \subseteq \bigcup_{i=1}^{|A|} R^i.$$

根据已给的关系 R，有一种确定的"方法"（不一定是"算法"）可以构造出它的"闭包"；构造闭包的运算，称为**闭包运算**．关于闭包运算，有下述重要的性质．

定理 3.3.23 设 R 是集合 A 上的二元关系．

(1) 若 R 是自反的，则 $s(R)$，$t(R)$ 都是自反的．

(2) 若 R 是对称的,则 $r(R)$, $t(R)$都是对称的.

(3) 若 R 是传递的,则 $r(R)$是传递的.

定理 3.3.24 设 R_1, R_2 都是 A 上的二元关系,则有

(1) $R_1 \supseteq R_2 \Rightarrow s(R_1) \supseteq s(R_2)$.

(2) $R_1 \supseteq R_2 \Rightarrow t(R_1) \supseteq t(R_2)$.

(3) $R_1 \supseteq R_2 \Rightarrow r(R_1) \supseteq r(R_2)$.

由定理 3.3.24 可以看出,求自反闭包、对称闭包和传递闭包的运算是保持单调性(在集合包含的意义上)的单调运算. 这表明闭包运算有良好的性质.

定理 3.3.25 设 R_1,R_2 都是 A 上的二元关系,则有

(1) $r(R_1 \cup R_2) = r(R_1) \cup r(R_2)$. (分配律)

(2) $s(R_1 \cup R_2) = s(R_1) \cup s(R_2)$. (分配律)

(3) $t(R_1 \cup R_2) \supseteq t(R_1) \cup t(R_2)$. (弱分配律)

定理 3.3.26 设 R 是 A 上的二元关系,则有

(1) $rs(R) = sr(R)$. (交换律)

(2) $rt(R) = tr(R)$. (交换律)

(3) $ts(R) \supseteq st(R)$. (弱交换律)

定理 3.3.26 中的 $rs(R) \triangleq r(s(R))$,是由关系 R 的对称闭包 $s(R)$所构成的自反闭包. 常称为关系 R 的**自反对称闭包**. 其余的 $rt(R)$,$ts(R)$分别称作关系 R 的**自反传递闭包**与**传递对称闭包**.

传递闭包和自反传递闭包,经常出现在形式语言与程序设计中,在计算机文献中常把 $t(R)$记作 R^+,把 $rt(R)$记作 R^*.

例 3.3.27 设 $\mathbf{Z}$ 是整数集,$<$是 $\mathbf{Z}$ 上的"小于"关系,则

$st(<) = s(<)$($=$ "$\neq$", 即"不相等" 关系).

$ts(<) = t(\neq)$.

由于 $t(\neq) \supseteq \neq$,因此有 $ts(<) \supseteq st(<)$.

3.4 等价关系与划分

在数学与计算机科学中，经常使用等价关系. 它是对“信息”与“数据”进行分类的一种普遍原则. 为了便于数学推导，经常用等价关系代替分类.

定义 3.4.1 集合 A 上的自反、对称和传递的关系，称为 A 上的**等价关系**(equivalent relation).

例 3.4.2 任意集合 A 上的恒等关系 I_A 是 A 上的等价关系.

例 3.4.3 整数集 $\mathbf{Z}$ 上的模 n 同余关系 R：

$$aRb \Leftrightarrow n \mid (a-b), \ (n \text{ 整除} (a-b)),$$

即 $a \equiv b(\bmod n)$ 是 $\mathbf{Z}$ 上的等价关系.

定义 3.4.4 设 R 是集合 A 上的等价关系，$x \in A$，称集合

$$[x]_R = \{y \mid x \in A \text{ 且} \langle x,y \rangle \in R\},$$

是 A 关于 R 的**等价类**(equivalence class). 符号$[x]_R$ 中的元素 x 称为该类的**生成元(或代表元)**(generator).

显然，当 $A \neq \varnothing$ 时，$[x]_R$ 是 A 上的非空子集，而且$[x]_R$ 中任何两个元素 a,b 均互相等价(即 a,b 有等价关系). 常记作 $a \underset{R}{\sim} b$，在不会混淆时记作 $a \sim b$. 此外，等价类中任何一个元素均可作为该类的生成元，而且等价类与生成元的选择无关.

例 3.4.5 设 R_3 是整数集 $\mathbf{Z}$ 上的模 3 同余关系，则 R_3 是等价关系.

$\mathbf{Z}$ 关于 R_3 的等价类是

$$[0]_{R_3} = \{x \mid x = 3n, \ n \in \mathbf{Z}\},$$

$$[1]_{R_3} = \{x \mid x = 3n+1, \ n \in \mathbf{Z}\},$$

$$[2]_{R_3} = \{x \mid x = 3n+2, \ n \in \mathbf{Z}\}.$$

等价类具有下面的重要性质.

定理 3.4.6 设 R 是 A 上的等价关系，则有

(1) $x \sim y \Leftrightarrow [x]_R = [y]_R$,

(2) $x \nsim y \Leftrightarrow [x]_R \cap [y]_R = \varnothing$.

该定理表明：集合 A 上关于等价关系 R 的等价类(集合)，或者二者重合，或者二者分离(即没有公共元素). 因此，集合 A 中的元素可按等价关系进行正确的"分类".

定义 3.4.7 设集合 A 的非空子集族 $\pi(A)$:

$$\pi(A) = \{A_\alpha \mid \alpha \in I,\ A_\alpha \subseteq A \text{ 且 } A_\alpha \neq \varnothing\},$$

满足

(1) $\bigcup_{\alpha \in I} A_\alpha = A$,

(2) $\alpha \neq \beta \Leftrightarrow A_\alpha \cap A_\beta = \varnothing$,

称 $\pi(A)$ 是集合 A 的一个**划分**(partition). A_α 称为划分 $\pi(A)$ 的**块**(block).

定义 3.4.8 设 R 是集合 A 上的等价关系，由 R 确定的等价类构成的集族，称为集合 A 上关于 R 的**商集**(quatient set)，记为

$$A/R = \{[x]_R \mid x \in A\}.$$

有些文献中记 $B = A/R$ 为 $A = B \oplus R$(形式上好像 A/R 等于 B，故称为商集).

集合 A 上的等价关系与集合 A 上的划分有紧密的联系：一旦给定集合 A 上的等价关系，就可以确定 A 上的一个划分(即可以把 A 中的元素按关系 R 进行分类，产生 A 上的划分 $\pi(A)$. 反之，给定集合 A 上的一个划分，则可以确定 A 上的一个等价关系. 这是对集合 A 中元素进行正确分类的重要原则. 它可以通过下述 3 个定理加以实现(定理 3.4.9～定理 3.4.11).

定理 3.4.9 设 R 是 A 上的等价关系，则可唯一确定 A 的划分：

$$\pi_R(A) = \{[x]_R \mid x \in A\}.$$

定理 3.4.10 设 $\pi(A)$ 是集合 A 的一个划分，则可唯一确定

A 上的一个等价关系：

$$R_\pi(A) = \{\langle x, y\rangle \mid x \in A \text{ 且 } x, y \text{ 属于 } \pi(A) \text{ 中同一块}\}.$$

定理 3.4.11 设 R_1, R_2 是集合上的等价关系，则有

$$R_1 = R_2 \Leftrightarrow A/R_1 = A/R_2.$$

等价关系对于集合的基本运算 $\cap$，$\cup$ 有下述性质.

定理 3.4.12 设 R_1, R_2 是 A 上的等价关系，则有

(1) $R_1 \cap R_2$ 是等价关系，

(2) $(R_1 \cup R_2)^+$ 是等价关系.

读者注意，除非 $R_1 = R_2$，一般情形 $R_1 \cup R_2$ 未必是等价关系. 但上面的定理 3.4.12 指出，不论 R_1 与 R_2 是否相同，$(R_1 \cup R_2)^+$ 一定存在，而且也是等价关系.

3.5 序关系与偏序集

3.5.1 引言

集合元素间的序关系与元素间的等价关系一样也是一种重要的关系. 根据等价关系可以对集合中元素进行严格的分类；根据序关系可以把集合中的元素恰当地排序. 有了一定的序关系才能够对多媒体数据库中的“信息”与“数据”进行“储存”，“加工”与“传输”. 序关系对于情报检索、数据处理、信息传输、程序运行等，极为重要.

定义 3.5.1 设 R 是集合 A 上的自反、反对称和传递关系，则称 R 是 A 上的**偏序关系**(partial ordering).

定义 3.5.2 设 R 是集合 A 上的反自反、传递关系，则称 R 是 A 上的**拟序关系**(quasi order relation).

读者注意，有些文献中称反自反、反对称与传递关系为拟序关系. 事实上可以证明：若 R 是定义 3.5.2 下的拟序关系，则 R 必

有反对称性. 因此,在定义拟序关系时,添加反对称性是多余的.

例 3.5.3 设 X 是任意集合,则它的幂集合 $\mathscr{P}(X)$ 上的包含关系($\subseteq$)是偏序关系;真包含关系($\subset$)是拟序关系.

由此可见,集合中的包含关系与真包含关系不可混淆.

例 3.5.4 实数域 $\mathbf{R}$ 上的"不大于"关系($\leqslant$)是偏序关系;"小于"关系($<$)是拟序关系.

3.5.2 偏序集的性质

定义 3.5.5 设关系$\leqslant$是集合 A 上的偏序关系,称集 A 关于$\leqslant$构成**偏序集**(partial order set),记作$\langle A,\leqslant\rangle$.

定义 3.5.6 设关系$<$是集合 A 上的拟序关系,称集 A 关于$<$构成**拟序集**(quasi order set),记作$\langle A,<\rangle$.

读者注意,把偏序关系记作$\leqslant$(把拟序关系记作$<$),并不是说所有偏序关系都是"不大于"关系(所有拟序关系都是"小于"关系). 事实上,由于实数域 $\mathbf{R}$ 上的"不大于"关系是一种典型的偏序关系("小于"关系是一种典型的拟序关系). 因此现今多数文献中常把偏序关系,拟序关系分别记作$\leqslant$与$<$.

显然$\langle\mathscr{P}(X),\subseteq\rangle$是偏序集,$\langle\mathscr{P}(X),\subset\rangle$是拟序集.

例 3.5.7 设关系$\leqslant$是集合 $\mathbf{N}$ 上的整除关系,则$\langle\mathbf{N},\leqslant\rangle$是偏序集.

例 3.5.8 设 $\Sigma=\{a,b,c,\cdots,x,y,z\}$(英文字母集),$\Sigma^*$ 中的元素是由 Σ 上的字母串组成的"字"(包括由"空格"组成的"空字"),Σ^* 上的关系$<$定义如下:

$w_1<w_2\Leftrightarrow w_1$ 是 w_2 的真子串(例如 of$<$off),则$\langle\Sigma^*,<\rangle$是拟序集.

定义 3.5.9 设$\langle A,\leqslant\rangle$是偏序集,若对于任意的 $x,y\in A$,总有 $x\leqslant y$ 或 $y\leqslant x$,则称$\langle A,\leqslant\rangle$是**全序集**(total order set).

由定义 3.5.9 可知,在实数集 $\mathbf{R}$ 中"不大于"关系$\leqslant$也是一种

全序关系. 即人们常说的:"任意两实数总可以比较大小的". 然而,对偏序集$\langle \mathscr{P}(A), \subseteq \rangle$而言,则不能说:"任意两集合,总是一个包含另一个". 这就是"全序"与"偏序"的本质差异. 仅当集合A是单元素集,或空集时,$\langle \mathscr{P}(A), \subseteq \rangle$才是全序集. 由几何直观上看,全序集中的元素均可以按序排列在一条直线上,因此,有些文献中称全序为"线性序".

为了深入地研究偏序集,现介绍下述概念.

定义 3.5.10 设$\langle A, \leqslant \rangle$是偏序集,对于任意的$x, y \in A$,若集合

$$[x,y] = \{z \mid \text{对任意的 } z \in A: x \leqslant z \text{ 且 } z \leqslant y\},$$

则称$[x,y]$为偏序集$\langle A, \leqslant \rangle$上的**区间**(interval).

读者注意,定义 3.5.10 中区间的定义与实数集 **R** 中区间的定义有所不同,它的含义更加广泛. 比如,当$x=y$时,$[x,y] \neq \varnothing$(而是一个单元素集$[x,y]=\{x\}=\{y\}$). 当$x \neq y$时,$[x,y]$也有可能是空集.

定义 3.5.11 设$\langle A, \leqslant \rangle$是偏序集,若$x, y \in A$满足

(1) $x \neq y$,

(2) $[x,y]=\varnothing$,

则称元素y**覆盖**(covering)元素x,或称y是x的**直接后继**(immediate successor),或称x是y的**直接先行**(immediate predecessor).

例 3.5.12 设$A=\{a,b\}$,在偏序集$\langle \mathscr{P}(A), \subseteq \rangle$中,元素$\varnothing$被元素$\{a\}$覆盖,也被元素$\{b\}$覆盖. 而元素$\{a,b\}$既覆盖$\{a\}$,也覆盖$\{b\}$.

在偏序集中,虽然$\varnothing \subseteq \{a,b\}$,但是由于区间$[\varnothing, \{a,b\}] \neq \varnothing$(因为元素$\{a\}$在区间内),所以$\{a,b\}$不覆盖$\varnothing$.

我们用图 3.4 表示. 这种图称为偏序集的 Hasse 图. 集合中的元素,均由图中的"结点"(或"顶点")表示. 元素间有偏序关系

者均有线段连接，无线段连接的结点，它所代表的元素间无偏序关系．Hasse 图是表示偏序集的一种“直观”方法．

例 3.5.13 设$\leqslant$是自然数集上的“不大于”关系，$\langle \mathbf{N}, \leqslant\rangle$是一个偏序集（同时也是全序集）．它的 Hasse 图是图 3.5．

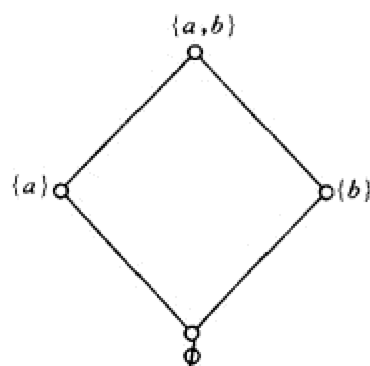


图 3.4



图 3.5

由图 3.5 可以看出$\langle \mathbf{N}, \leqslant\rangle$中的元素可以排列在一条“直线”上．

例 3.5.14 设集合 $A=\{1,2,3,4,5,6,7\}$，D 是 A 上的整除关系，则偏序集$\langle A, D\rangle$的 Hasse 图是图 3.6．

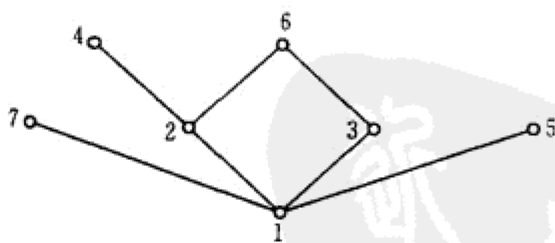


图 3.6

例 3.5.15 设集合 $A=\{a,b,c\}$，则$\langle \mathscr{P}(A), \subseteq\rangle$是偏序集，它的 Hasse 图是图 3.7．

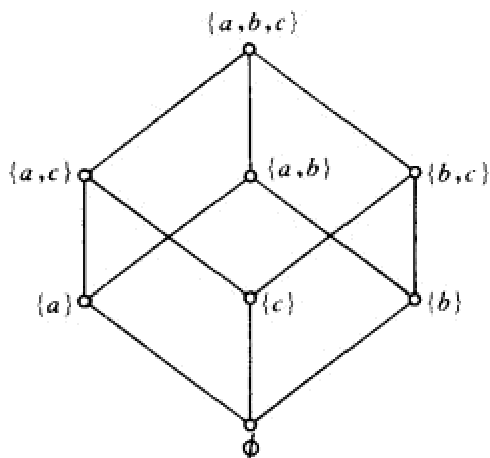


图 3.7

定义 3.5.16 设$\langle A,\leqslant\rangle$是偏序集,若存在$a\in A$,使得对任意的$x\in A$,有

$$x\leqslant a,$$

则称元素a为$\langle A,\leqslant\rangle$的**最大元(素)**(greatest element). 类似地可定义**最小元(素)**(smallest element).

注 对偏序集而言不一定有最大元,如例 3.5.13 与例 3.5.14 就没有最大元,但可能有最小元. 在图 3.6 中的结点 4,5,6,7 均可以算作是"局部"最大元. 这种元素称为极大元. 而 1 则是最小元(也是极小元).

定义 3.5.17 设$\langle A,\leqslant\rangle$是偏序集,若存在$a\in A$,使得对任意的$x\in A$满足

$$a\leqslant x\Rightarrow x=a,$$

则称a为$\langle A,\leqslant\rangle$的**极大元**. 类似地可定义**极小元**.

一般情形,极大元不一定是最大元,而最大元显然是极大元. 特别,全序集的极大元一定是最大元. 然而,对偏序集而言,它的极大元(极小元),最大元(最小元)并不一定存在.

类似于子集概念,对于偏序集而言,也有子偏序集的概念. 显

然，偏序集的任何子集，仍为一偏序集.

下面介绍有关的重要概念.

定义 3.5.18 设$\langle A,\leqslant\rangle$是偏序集，$B\subseteq A$，$a\in A$. 若对于任意的$x\in B$，$x\leqslant a$，则称元素$a$是子偏序集$\langle B,\leqslant\rangle$的**上界**(upper bound). 类似地，可定义**下界**(lower bound).

例 3.5.19 在偏序集$\langle\mathscr{P}(\{a,b\}),\subseteq\rangle$中，对于子偏序集$\langle\{\{a\},\{b\},\varnothing\},\subseteq\rangle$，元素$\{a,b\}\in\mathscr{P}(\{a,b\})$是它的上界. 元素$\{a\}$，$\{b\}$均为该子偏序集的极大元，它本身没有最大元. $\varnothing$是它的极小元，同时也是它的最小元，也是它的下界.

对于子偏序集$\langle\{\{a\},\varnothing\},\subseteq\rangle$，元素$\{a,b\}$，$\{a\}$均为它的上界，而$\{a\}$是它的最小上界(同时也是它的最大元(见图 3.4). 因此还有下面重要概念.

定义 3.5.20 设$\langle A,\leqslant\rangle$是偏序集，$B\subseteq A$，若元素$\overline{m}\in A$是$\langle B,\leqslant\rangle$的最小上界，则称$\overline{m}$是$\langle B,\leqslant\rangle$的**上确界**(least upper bound)，记为$\overline{m}=\sup B$. 类似地，$\langle B,\leqslant\rangle$的最大下界$\underline{m}$称为$\langle B,\leqslant\rangle$的**下确界**(great lower bound)，记为$\underline{m}=\inf B$.

例 3.5.21 设偏序集$\langle\{2,3,4,6,8,9,10\},D\rangle$，其中$D$是整除关系，则偏序集$\langle\{4,6\},D\rangle$有一个下确界(为 2)，它没有上确界. 偏序集$\langle\{2,3,4,6\},D\rangle$既没有上界，也没有下界(见图 3.8).

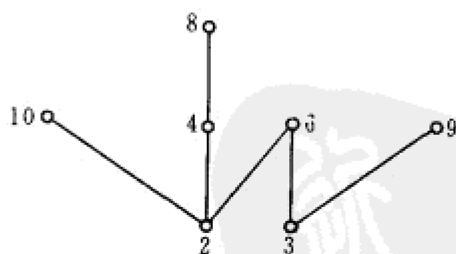


图 3.8

4　映射(函数)

4.1　映射(函数)的概念

映射(函数)在现代数学中是一种极其重要的概念. 在不同的场合,有不同的称呼,因此映射(mapping/map)、函数(function)、对应(correspondance)、变换(transformation)、算子(operator)、函子(functor),在某种意义上说都是一种同义词. 在现代文献中,使用最多的是映射与函数.

函数一词最早为 Leibniz 在 1694 年所使用,现代常用的函数记号 $f(x)$是 1734 年由 Clairaut 及 Euler 所使用. 函数这个词在近代科学中有非常广泛的意义.

在现代数学中,集合、关系、函数三个重要概念是紧密相联的,在连续数学中常常从集合与函数谈起,在离散数学中常常从集合与关系谈起,从函数概念出发可以定义关系概念;反之,从关系概念出发也可以定义函数概念. 在离散数学中,经常用集合或关系概念来定义函数概念.

定义 4.1.1　设关系 $R\subseteq X\times Y$ 满足以下条件:对于任意的 $x\in X$, y, $z\in Y$:

$$\langle x,y\rangle \in R \text{ 且} \langle x,z\rangle \in R \Rightarrow y = z,$$

则称关系 R 为**函数**(function).

依照传统,常把函数用小写拉丁字母或希腊字母表示,记作:$f,g,h,\cdots$或 $\varphi,\psi,\cdots$. 于是有

$$\langle x,y\rangle \in f \Leftrightarrow y = f(x) \text{ 或 } f(x) = y.$$

因此,函数是一种特殊的关系.

用现代数学的记号常表示为：

$$f: X \longrightarrow Y \quad (\text{或 } X \xrightarrow{f} Y)$$

或者 $$f: x \longmapsto y \quad (\text{或 } x \longmapsto f(x))$$

$$x \in X, \ y \in Y$$

对于函数有定义域与值域的概念.

定义 4.1.2 若 $f \subseteq X \times Y$ 是函数，下述集合

$\mathrm{dom} f = \{x \mid x \in X$，存在 $y \in Y$，使得 $\langle x, y \rangle \in f\}$，

$\mathrm{ran} f = \{y \mid y \in Y$，存在 $x \in X$，使得 $\langle x, y \rangle \in f\}$，

则称 $\mathrm{dom} f$ 是 f 的**定义域**(domain). $\mathrm{ran} f$ 是 f 的**值域**(range/codomain).

注意，$\mathrm{dom} f \subseteq X$，$\mathrm{ran} f \subseteq Y$，其中的元素与 f 中的元素是不同的.

定义 4.1.3 设 $f \subseteq X \times Y$.

(1) $\mathrm{dom} f = X$，则称 f 是 X 上的**全函数**(total function)；

(2) $\mathrm{dom} f \subset X$，则称 f 是 X 上的**偏函数**(partial function).

一般情形，f 可能是 X 上的偏函数，但 f 必是 $\mathrm{dom} f$ 上的全函数. 在连续数学中，常在 $\mathrm{dom} f$ 中对函数进行研究，所以它所研究的函数大多是全函数，因此没有介绍偏函数的概念. 而在离散数学中，就必须区分这两种概念.

从 X 到 Y 的全体全函数构成的集合记作 ${}^XY$，从 X 到 Y 的全体偏函数构成的集合记作 ${}^{X}\!Y$，它们之间的关系是

$$f \in {}^{X}\!Y \Leftrightarrow \underset{X_1 \subset X}{\exists} f \in {}^{X_1}Y.$$

通常全函数又称为全映射，偏函数亦称为偏映射. 然而，从函数的定义看，$X \times Y$ 的子集中只有一部分子集可以用来定义函数.

定义 4.1.4 若从 X 到 Y 的映射 f，使得 X 中不同的元素有 Y 中不同的元素与之对应，换言之，当 $x_1 \neq x_2$ 时，$f(x_1) \neq f(x_2)$，则称 f 是**单射**(injective)或 1-1 **映射**(one to one mapping)（有些

文献称单射为“内射”).

定义 4.1.5 若 f 是从 X 到 Y 的映射,满足

$$\operatorname{ran} f = Y,$$

则称 f 是从 X 到 Y **上的映射**,或称 f 是**满射**(surjective).

定义 4.1.6 设 f 是从 X 到 Y 的映射,若 f 既是单射又是满射,则称 f 是**双射**(bijective).

与关系一样,对于映射,也有限制与扩张的概念.

定义 4.1.7 设 $f: X\to Y$, $S\subseteq X$, 若 $\varphi: S\to Y$, 满足:对所有的 $x\in S$: $\varphi(x)=f(x)$,则称 φ 是 f 在 S 上的一个**限制**(restriction),记作 $f\upharpoonright S$.

定义 4.1.8 设函数 $\varphi: S\to T$, $S\subseteq X$, $T\subseteq Y$, 若函数 $f: X\to Y$ 满足:对所有的 $x\in S$, $f(x)=\varphi(x)$, 则称 f 是 φ 在 X 上的一个**扩张**(extension),记作 $f=\mathrm{Ext}\varphi$.

例 4.1.9 设函数 $\varphi: X\to Y$, 其中 $X=\{0,2,4,6,8\}$, $Y=\{a,b,c,d,e,f,g\}$.

φ 定义如下:$\varphi(2)=a$, $\varphi(4)=b$, $\varphi(6)=d$, $\varphi(8)=c$(如图 4.1).

可以看出,φ 是从 X 到 Y 的单射,是偏函数.

$$\operatorname{dom}\varphi=\{2,4,6,8\}\subset X,$$
$$\operatorname{ran}\varphi=\{a,b,c,d\}\subset Y,$$

例 4.1.10 设 $X=\{a,b,c,d,e\}$, $Y=\{1,2,3,4,5\}$.

$f: X\to Y$ 定义如下:

$$f=\{\langle a,1\rangle, \langle b,2\rangle, \langle c,2\rangle, \langle d,3\rangle\}.$$

$g: X\to Y$ 定义如下:

$$g=\{\langle a,1\rangle,\langle b,3\rangle,\langle c,4\rangle,\langle d,2\rangle,\langle e,5\rangle\}.$$

显然 f 是偏函数,它不是单射,也不是满射. 而 g 既是单射,又是满射,所以 g 是双射,且 g 是全函数.

例 4.1.11 设函数 f: $\mathbf{R}\to\mathbf{C}$,对于一切 $x\in\mathbf{R}$:

$$f(x) = \mathrm{i}\,|x| \quad (\mathrm{i}\ 是虚单位, \mathrm{i}^2 = -1).$$

显然 f 既不是单射,也不是满射.

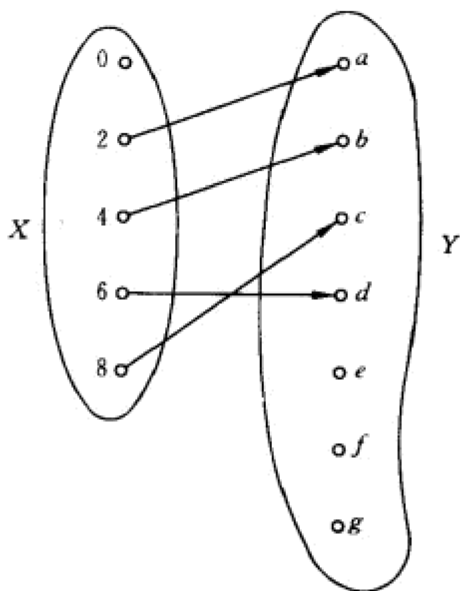


图 4.1

4.2 复合映射与逆映射

设函数 $g: X \to Y$, $f: Y \to Z$, 则有从 X 到 Z 的复合关系,可以证明这个复合关系是一个函数(见图 4.2).

定义 4.2.1 设函数 $g: X \to Y$, $f: Y \to Z$, 则称函数 $h: X \to Z$:

$$h = \{\langle x,z \rangle \mid x \in X,\ z \in Z\ 且存在\ y \in Y\ 使得\ \langle x,y \rangle \in g\ 且 \langle y,z \rangle \in f\}$$

是从 X 到 Z 的**复合函数**(composite function),或**复合映射**(composite mapping). 记作 $h = f \circ g$.

读者注意,按复合关系的记号(定义 3.2.14)定义 4.2.1 中的关系 h 应该记作:

$$h = g \circ f,$$

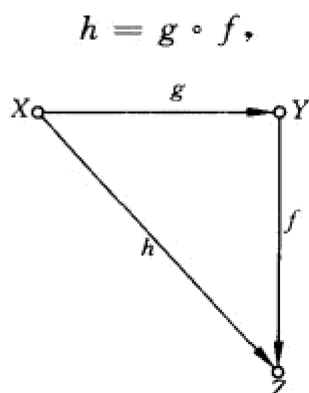


图 4.2

从而有

$$\begin{aligned} h(x) &= (g \circ f)(x) \\ &= f(g(x)). \end{aligned}$$

按传统记法复合函数 $h(x) = f(g(x))$. 这与 $h(x) = (g \circ f)(x)$的记法有所不同,复合函数中函数符号出现的次序就不一致. 为了避免这种麻烦,就一律记复合函数为: $h = f \circ g$, 这样一来,就有

$$\begin{aligned} h(x) &= (f \circ g)(x) \\ &= f(g(x)). \end{aligned}$$

因此,应留意在关系与函数间施行复合运算时,在符号的书写方面有"次序"的差别.

此外,在定义 4.2.1 中,还隐含假定: $\mathrm{dom} f \cap \mathrm{ran} g \neq \varnothing$, 否则 $f \circ g$ 是空关系.

例 4.2.2 若 $f(x) = x+2$, $g(x) = x^2$ 为定义在 $\mathbf{R}$ 上的实函数,则 $f \circ f$, $g \circ f$, $f \circ g$, $g \circ g$ 如下.

$(f \circ f)(x) = f(f(x)) = f(x+2) = (x+2)+2 = x+4.$

$(f \circ g)(x) = f(g(x)) = f(x^2) = x^2 + 2.$

$(g \circ f)(x) = g(f(x)) = g(x+2) = (x+2)^2 = x^2 + 2x + 4.$

$$(g \circ g)(x) = g(g(x)) = g(x^2) = (x^2)^2 = x^4.$$

可以看出在此例中 $f \circ g \neq g \circ f$，交换律不成立.

例 4.2.3 设 $X=\{1,2,3,4\}$，g 和 f 均为 $X \to X$ 的函数，定义如下：

$$g = \{\langle 1,2\rangle, \langle 2,1\rangle, \langle 3,3\rangle, \langle 4,1\rangle\},$$
$$f = \{\langle 1,2\rangle, \langle 2,3\rangle, \langle 3,1\rangle\},$$

则有

$$f \circ g = \{\langle 1,3\rangle, \langle 2,2\rangle, \langle 3,1\rangle, \langle 4,2\rangle\}.$$
$$g \circ f = \{\langle 1,1\rangle, \langle 2,3\rangle, \langle 3,2\rangle\}.$$
$$f \circ f = \{\langle 1,3\rangle, \langle 2,1\rangle, \langle 3,2\rangle\}.$$
$$(f \circ f) \circ f = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle\}.$$
$$f \circ (f \circ f) = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle\}.$$

由例 4.2.2，例 4.2.3 可以看出，函数的复合不一定满足交换律，但一定满足结合律.

关于复合映射，有下列重要性质.

定理 4.2.4 设 $g: X \to Y$，$f: Y \to Z$，$h: Z \to W$，则有 $k: X \to W$：

$$(h \circ f) \circ g = h \circ (f \circ g) \quad (= k).$$

见图 4.3，图 4.4.

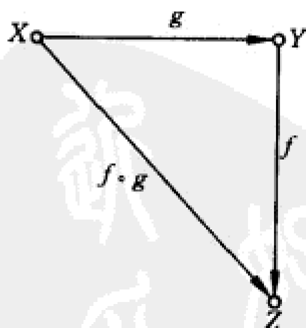


图 4.3

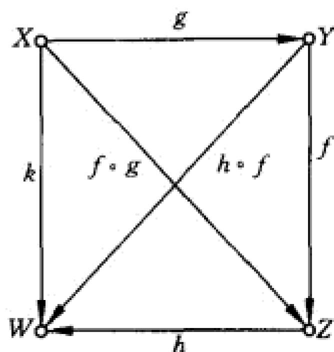


图 4.4

定理 4.2.5 设 $g: X\to Y$，$f: Y\to Z$，则有

(1) 若 f，g 均为满射，则 $f\circ g$ 是满射.

(2) 若 f，g 均为单射，则 $f\circ g$ 是单射.

(3) 若 f，g 均为双射，则 $f\circ g$ 是双射.

上述定理表明，复合运算"∘"对于满射、单射、双射具有"保持性". 但上述定理的逆不恒真.

定理 4.2.6 设 $g: X\to Y$，$f: Y\to Z$，$f\circ g: X\to Z$，则有

(1) 若 $f\circ g$ 是满射，则 f 是满射.

(2) 若 $f\circ g$ 是单射，则 g 是单射.

(3) 若 $f\circ g$ 是双射，则 f 是满射，g 是单射.

现在研究逆映射. 对于任意的关系 R，它的逆关系 R^{-1} 总是存在的. 但作为特殊关系的映射，它的逆关系并不一定是映射，因此映射的逆映射并非总是存在的.

定义 4.2.7 设函数 $f: X\to Y$. 若存在 $y\in Y$，使得对一切 $x\in X$，有 $f(x)=y$，则称 f 是**常函数**(constent function).

定义 4.2.8 设函数 $f: X\to Y$. 若对一切 $x\in X$，有 $f(x)=x$，则称 f 是 X 上的**恒等函数**(identity function)，记作 I_X.

由于在一般情况下，复合运算没有交换性质，即 $f\circ g\neq g\circ f$，因此有左(右)逆映射的定义.

定义 4.2.9 设 $g: X\to Y$, $f: Y\to Z$. 若 $g\circ f=I_Y$ ($f\circ g=I_X$), 则称 g 是 f 的**左(右)逆映射**(left(right) inverse mapping). 这时称 f 为**有左(右)逆映射**.

关于逆映射有下列重要性质.

定理 4.2.10 设 $f: X\to Y$, 且 $X\neq\varnothing$, 则有

(1) f 有左逆(映射)$\Leftrightarrow f$ 是单射.

(2) f 有右逆(映射)$\Leftrightarrow f$ 是满射.

(3) f 有逆(即 f 既有左逆,又有右逆)$\Leftrightarrow f$ 是双射.

定理 4.2.11 设 $f: X\to Y$, $g: Y\to X$, 则有

(1) 若 $g\circ f=I_X$, 则 f 是单射, g 是满射.

(2) 若 $f\circ g=I_Y$, 则 f 是满射, g 是单射.

定理 4.2.12 设 $f: X\to Y$, $g: Y\to X$, 则 f, g 均为双射的充要条件是 f, g 满足:

$$\begin{cases} g\circ f=I_X, \\ f\circ g=I_Y. \end{cases}$$

定理 4.2.13 设 $f: X\to Y$, $g: Y\to X$, 若 f, g 满足

$$\begin{cases} g\circ f=I_X, \\ f\circ g=I_Y. \end{cases}$$

则 $g=f^{-1}$, 且 $f=g^{-1}$.

定理 4.2.14 若 $f: X\to Y$ 是双射,则$(f^{-1})^{-1}=f$.

定理 4.2.15 设 $g: X\to Y$, $f: Y\to Z$ 都是双射,则有

$$(f\circ g)^{-1}=f^{-1}\circ g^{-1}.$$

4.3 函数概念的拓展

由于应用与理论方面的需要,函数概念有进一步拓展. 函数中自变量不仅仅是某集合中的元素,自变量本身就可以是集合(换言之,可以在 $\mathscr{P}(A)$上定义函数),而且它们的值,也可以是集合.

主要有下列 4 种类型的函数.

(1) 函数的自变量是集合,它的值是实数. 常见的为微积分学中的"区间上的定积分"图(4.5):

$$S(I) = \int_I f(x)\mathrm{d}x.$$

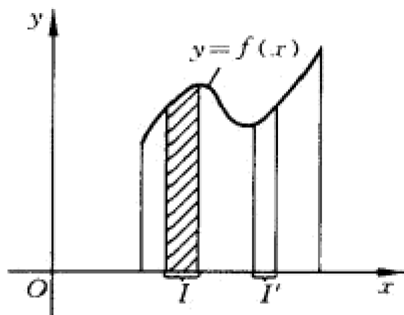


图 4.5

$S(I)$是集合 I(现在是区间)上的函数. 一般称 $S(I)$是**集函数**(set function). 如面积函数,体积函数等.

(2) 函数的自变量是实数(或复数),而它的值是集合(通常是 **R**/**C** 中的子集). 常见的是分析数学中的多值函数. 一般称为**集值函数**(set value function).

这种函数,近年来在信息论、博奕论(对策论)与经济数学中大量出现.

(3) 函数的自变量也是函数,它的值是实数(或复数). 这种函数在近代文献中统称为**泛函数**(functional)(见本手册《现代应用分析卷》).

(4) 函数的自变量是函数,它的值也是函数(实函数或复函数),这种函数在近代文献中统称为**算子**(operator)(见本手册《现代应用分析卷》).

以上 4 种类型的函数,都可以概括为从集合到集合的函数. 事实上,在(1),(2)中当自变量或函数所取之值是实数时,它本身

可以看做是以自身为元素的单元素集. 在(3),(4)中当自变量或函数值均为函数时,情况完全类似. 其实,函数是一种特殊的关系,而关系又是一种特殊的集合,所以函数也是一种集合.

函数概念可以拓展到变元为集合的场合,这样就有像集与逆像集的概念.

定义 4.3.1 设 $f: X \to Y$, $A \in \mathscr{P}(X)$,则称

$$f(A) = \{y \mid \text{存在 } x \in A, \text{ 使得 } f(x) = y\}$$

为集合 A 在 f 作用下的**像集**(image set).

定义 4.3.2 设 $f: X \to Y$, $B \in \mathscr{P}(Y)$, 则称

$$f^{-1}(B) = \{x \mid \text{存在 } y \in B \text{ 使得}, f(x) = y\}$$

为集合 B 在 f^{-1}作用下的**逆像集**(inverse image set).

关于像集与逆像集,有下面重要的性质.

定理 4.3.3 设 X,Y 是任意的集合,$A,B \in \mathscr{P}(X)$, 映射 $f: X \to Y$, 则有

(1) $f(A \cup B) = f(A) \cup f(B)$;

(2) $f(A \cap B) \subset f(A) \cap f(B)$;

(3) $f(A) \setminus f(B) \subset f(A \setminus B)$;

(4) $A \subset f^{-1}(f(A)) \quad (= (f^{-1} \circ f)(A))$;

(5) $A \subset B \Rightarrow f(A) \subset f(B)$.

推论 4.3.4 仅当 f 是单射时,才有

$$f(A \cap B) = f(A) \cap f(B).$$

定理 4.3.5 设 X,Y 是任意的集合,$A,B \in \mathscr{P}(Y)$, 映射 $f: X \to Y$, 则有

(1) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$;

(2) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;

(3) $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$;

(4) $f(f^{-1}(A)) = A \cap f(X)$;

$(f \circ f^{-1})(A) = A \cap f(X)$;

(5) $A\subset B\Rightarrow f^{-1}(A)\subset f^{-1}(B)$.

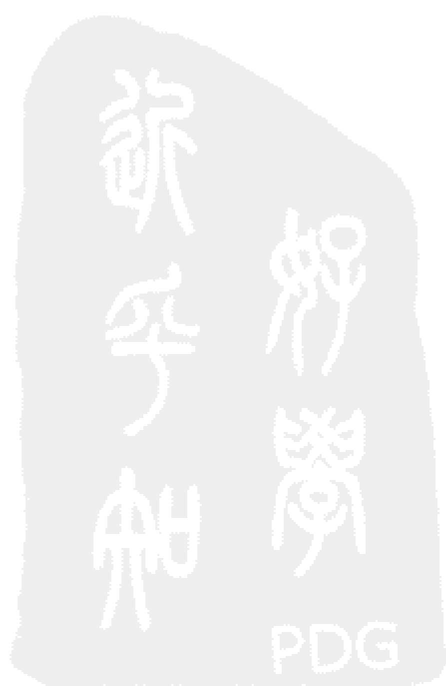
由定理 4.3.3 和定理 4.3.5 可知，在一般情形下，有

$$(f\circ f^{-1})(A)\subset A\subset (f^{-1}\circ f)(A).$$

推论 4.3.6 仅当 f 是满射时，才有

$$(f\circ f^{-1})(A)=f(f^{-1}(A))=A.$$

这里映射 f,f^{-1} 就是作用在集合上的“算子”. 而且算子 f^{-1} 较之算子 f 有更好的性质：它对集合的“包含”，“并”，“交”，与“差”运算，有保持性(见定理 4.3.5).



5 集合的基数

前面所研究的集合，有些集合的元素是有限的，有些则有无限多个元素. 但是我们没有一般地谈论集合中元素的多少；换言之，我们没有全面地考虑集合的"规模". 本章将对此详细叙述.

5.1 有限集与无限集

当抽象地研究集合时，本质上要考虑的是集合的"规模"，粗略地说就是"大小". 任意两个集合，它们的"大小"是否相同？哪一个集合的元素"较多"？

由有限个元素构成的集合，它的"规模"决定于集合中元素的"个数". 如果集合 A 和集合 B 中元素的"个数"相同，就称集合 A 和集合 B 的基数相同. 这时集合 A 和集合 B 之间可以建立起一一映射. 但是，对于由无限个元素构成的集合，"元素的个数"就没有确切的含义. 只有用基数相同的概念来刻画集合的"大小".

定义 5.1.1 设 A,B 是任意两集合，若存在双射 $f: A\to B$，则称集合 A 与集合 B **对等(或等势)**(equipotent)，记作 $A\sim B$；或称 A,B 的**基数相同**，记作 $|A|=|B|$(或 $\overline{\overline{A}}=\overline{\overline{B}}$).

例如，设 $A=\{0,1,2\}$，$B=\{a,b,c\}$，则 $A\sim B$ 或 $|A|=|B|$. 就有限集而言，"基数相同"和"有相同的基数"这两个概念是完全一样的. 并且有 $|A|=|B|=3$. 特别地，对有限集而言，它所含有的元素"个数"，就是它的基数.

定义 5.1.2 设 A 为集合，若 A 与集合 $\{0,1,2,\cdots,n-1\}$ 对等，则称 A 为**有限集**(finite set)，且 $|A|=n$. 若 A 不是有限集，则称它是**无限集**(infinite set).

定义 5.1.3 设 $A=\varnothing$，称 A 为有限集，且 $|\varnothing|=0$.

定理 5.1.4 自然数集合 $\mathbf{N}$ 是无限集.

没有一个自然数能作为 $\mathbf{N}$ 的基数. 以后记 $|\mathbf{N}|=\aleph_0$(读作：阿列夫零). 它是最小的无限基数.

例 5.1.5 Galileo 悖论(Galileo paradox) 设 $\mathbf{N}^+=\{1,2,\cdots,n,\cdots\}$，$\mathbf{N}^{(2)}=\{1,4,9,\cdots,n^2,\cdots\}$ 问 $\mathbf{N}^{(2)}\subseteq\mathbf{N}^+$? 还是 $\mathbf{N}^{(2)}\supseteq\mathbf{N}^+$?

G. Cantor 借助于等势的概念解决了这个"悖论".

由于在 $\mathbf{N}^+$ 与 $\mathbf{N}^{(2)}$ 之间存在着双射(即 $f:\mathbf{N}^+\to\mathbf{N}^{(2)}$，$n\mapsto n^2$)，因此，$\mathbf{N}^+$ 与 $\mathbf{N}^{(2)}$ 的元素"个数"是相等的.

显然有 $\mathbf{N}^{(2)}\subset\mathbf{N}^+$. 就是说 $\mathbf{N}^+$ 可以与它的一个真子集对等.

定理 5.1.6 无限集必与它的一个真子集对等.

推论 5.1.7 凡不能与自身的任意一个真子集对等的集合必为有限集(即不是无限集).

定理 5.1.6 揭示了无限集的一个重要的特征，即无限集可以与它的一个真子集对等，而对有限集来说这是不可能的. 因此，有些文献中采用定理 5.1.6 作为无限集的定义(这个定义首先由 Dedekind 提出).

5.2 可列集与不可列集

可列集是无限集合中最重要的集合.

定义 5.2.1 设任意集合 A，若存在从 $\mathbf{N}$ 到 A 的双射 $f:\mathbf{N}\to A$，则称 A 为**可列无限集**(countably infinite set)简称**可列集**(或**可数集**). 且记 $|A|=\aleph_0$.

上述定义表明，自然数集 $\mathbf{N}$ 可以排列成一个无穷序列的形式：0,1,2,3,4,…因此任何可列集中的元素也可以排成无穷序列的形式：$a_0,a_1,a_2,a_3,a_4,\cdots$. 反之，一集合中的元素可以排成无穷序列的形式，则该集合一定是可列集. 所以一个集合是可列集的

充要条件是：它的元素可以（按一定的规则）排成一个无穷的序列. 这是一个重要的直观概念. 下面介绍可列集的重要性质.

定理 5.2.2 任意无限集，必含有一个可列子集.

定理 5.2.3 可列集的任意无限子集必为可列集.

由定理 5.2.2 和定理 5.2.3 可知，可列集是无限集合中“最小者”.

定理 5.2.4 可列集中添加（删除）有限个元素后，仍为可列集.

定理 5.2.5 有限个可列集的并集仍为可列集.

定理 5.2.6 可列个可列集的并集仍为可列集.

证明 设可列个可列集排列如下：$A_1, A_2, A_3, \cdots$ 且两个互不相交，

$$
\begin{aligned}
A_1 &= \{a_{11}, a_{12}, a_{13}, a_{14}, \cdots, a_{1n}, \cdots\}, \\
A_2 &= \{a_{21}, a_{22}, a_{23}, a_{24}, \cdots, a_{2n}, \cdots\}, \\
A_3 &= \{a_{31}, a_{32}, a_{33}, a_{34}, \cdots, a_{3n}, \cdots\}, \\
A_4 &= \{a_{41}, a_{42}, a_{43}, a_{44}, \cdots, a_{4n}, \cdots\}, \\
&\cdots\cdots
\end{aligned}
$$

设 $A=\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup A_4 \cup \cdots$. 将 A_i 中的元素排列成下面的方阵.

$$
\begin{array}{cccc}
a_{11} \rightarrow a_{12} & & a_{13} \rightarrow a_{14} \cdots \\
\swarrow & \nearrow & \swarrow & \\
a_{21} & a_{22} & a_{23} & a_{24} \cdots \\
\downarrow \;\nearrow & \swarrow & & \\
a_{31} & a_{32} & a_{33} & a_{34} \cdots \\
\swarrow & & & \\
a_{41} & a_{42} & a_{43} & a_{44} \cdots \\
\downarrow & & & \\
\cdots\cdots & & &
\end{array}
$$

依照上面方阵中由“折线”所确定的对应关系，可把 A 中的元素排列如下：

a_{11}，a_{12}，a_{21}，a_{31}，a_{22}，a_{13}，a_{14}，a_{23}，a_{32}，a_{41}，…

所以 A 是可列集合.

定理 5.2.6 的证明中所采用的方法，由 G. Cantor 首创，称为 Cantor **折线法**，是一种重要的方法. 在理论计算机科学中广泛地使用.

例 5.2.7 下列诸集，均为可列集.

(1) $^n\mathbf{N}=\underbrace{\mathbf{N}\times\mathbf{N}\times\cdots\times\mathbf{N}}_{n}$.

(2) $\mathbf{Z}$.

(3) $\mathbf{Z}\times\mathbf{Z}$, $^n\mathbf{Z}$.

(4) $\mathbf{Q}$.

(5) $\mathbf{Q}\times\mathbf{Q}$, $^n\mathbf{Q}$.

(6) $\Sigma=\{a,b,\cdots,x,y,z\}$，$\Sigma$ 上所有的有限非空字符串的集合 Σ^+，Σ^+ 也是可列集.

以集合 $\mathbf{N}$,$\mathbf{Z}$ 为代表的集(还有 $^2\mathbf{N}$, $^2\mathbf{Z}$, $^3\mathbf{N}$, $^3\mathbf{Z}$)均为可列集，这是一类很重要的集合，它们在数据处理、形式语言学、计算机图形、图像学、数学形态学中有广泛的应用，常称它们为“数字空间”.

由例 5.2.7 可知，全部可用英文写成的书的集合；全部可用任意给定的程序语言写成的程序集合，都是可列的.

但是，无限集合中不仅仅只有可列集，有许多集合，例如 $\mathbf{R}$ 中的区间[0,1]中全体实数，就不是可列集.

定理 5.2.8 $\mathbf{R}$ 的子集[0,1]，是不可列集.

证明 由于[0,1]内的一切实数都可以用一个十进制的纯小数唯一地表示；对于有限小数，也记成无限小数的形式；例如

$$0.482$$

一律记作：

$$0.48199\cdots,$$

于是[0,1]由一个实数与一个十进制的无限纯小数一一对应．现在应用反证法．

若[0,1]内所有实数构成的集合是可列集，那么其中的元素必与 **N** 中的元素一一对应，于是就可以排成无穷序列：$x_1, x_2, \cdots, x_i, \cdots$．假设 x_i 的小数形式是 $0.x_{i1}x_{i2}\cdots x_{ij}\cdots(i,j=1,2,\cdots)$．其中 x_{ij} 是数字：0,1,2,…,9 中的某一个，即 $x_{ij}\in\{0,1,2,3,4,5,6,7,8,9\}$．现在把 $x_1, x_2, \cdots$ 竖排如下：

$$\begin{array}{lllll}
x_1 = 0.x_{11} & x_{12} & x_{13} & x_{14} & \cdots \\
 & \diagdown & & & \\
x_2 = 0.x_{21} & x_{22} & x_{23} & x_{24} & \cdots \\
 & & \diagdown & & \\
x_3 = 0.x_{31} & x_{32} & x_{33} & x_{34} & \cdots \\
 & & & \diagdown & \\
x_4 = 0.x_{41} & x_{42} & x_{43} & x_{44} & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots\diagdown
\end{array}$$

于是[0,1]中所有的实数均已在表中列出．换言之，任意纯小数一定出现于上表中的某一行（例如 $x_3=0.x_{31}x_{32}x_{33}x_{34}\cdots$）．

但是 Cantor 指出：按对角线构造一个新的小数 x^* 如下：

$$x^* = 0.x_{11}^*x_{22}^*x_{33}^*\cdots x_{nn}^*\cdots$$

使得

若 $\quad x_{nn}=5$，则令 $x_{nn}^*\neq 5$，

$\quad\quad x_{nn}\neq 5$，则令 $x_{nn}^*=5$．

显然 x^* 是一个纯小数，所以 $x^*\in[0,1]$．可是 x^* 绝不出现于上述表中．因为它与表中任何一个小数至少有一位数字相异，即 $x^*\notin[0,1]$．于是产生矛盾．

定理 5.2.8 证明[0,1]中所有实数，构成了一个不可列集．从而表明，并非所有无限集都是可列集，无限集也是有区别的．

定理 5.2.8 的证明中，Cantor 提出的用对角线元素构造小数 x^* 的方法，称为 **Cantor 对角线法**(Cantor diagonal method). 这种著名的方法后来有种种"变型". 它已成为现代数学与计算机科学中证明"否定性结论"的强有力工具. 例如，由 Cantor 对角线法可以证明："对于任何程序语言，必定存在一个数学上可以严格定义的函数，它的函数值不能用该程序语言所定义的任何程序计算出来"(参看例 5.3.20).

R 中的区间[0,1]，它的基数记为 $\aleph$，有时也记作 c；集合[0,1]也称为**连续统**(continuum).

定理 5.2.9 设 $a,b\in\mathbf{R}$ 且 $a<b$，则集合(区间)$[a,b]$，(a,b)，$[a,b)$，$(a,b]$的基数都是 $\aleph$.

定理 5.2.10 实数集 **R** 的基数 $|\mathbf{R}|=\aleph$.

定理 5.2.11 无理数集的基数是 $\aleph$.

定理 5.2.10 与定理 5.2.11 的结论是惊人的，初看起来无理数寥寥无几(例如 π，e，$\sqrt{2}$，…)，而人们通常接触的大多数都是有理数. 然而从理论高度揭示出实数集 **R** 中的无理数较之有理数要多得多！(事实上，绝大多数不循环的无穷小数都是无理数！)

定理 5.2.12 设 A 是有限集或可列集，B 是任意的无限集，则有 $|A\cup B|=|B|$.

读者注意，定理 5.2.12 指明，即使 $A\cap B=\varnothing$，结论仍然成立. 这就表明，在无限集中，可列集的基数是最小的.

5.3 集合的基数

5.3.1 基数的比较

利用双射的概念，给出了两集合的"基数相同"的严格定义. 现在给出集合"基数"的严格定义，以及它的种种性质.

定义 5.3.1 所有与集合 M 对等的集所构成的类(class)的共同性质,称为 M 的**基数**(cardinal number),记作 $|M|$(或 $\overline{\overline{M}}$, card$M$).

定义 5.3.2 若 $A \subseteq B$,则称 $|A| \leqslant |B|$;若 $|A| \leqslant |B|$ 且 $|A| \neq |B|$,则称 $|A|$ 小于 $|B|$. 记作 $|A| < |B|$.

下面给出有关集合基数的各种性质.

定理 5.3.3 设 A,B,C 为任意集,则有

(1) $A \sim A$;

(2) $A \sim B \Leftrightarrow B \sim A$;

(3) $A \sim B$ 且 $B \sim C \Rightarrow A \sim C$.

定理 5.3.4 设 A,B 为有限集,则 $A \sim B$ 的充要条件是 A,B 有同样多的元素。

定理 5.3.5 设 A,B,C 为任意集,则有

$$|A| \leqslant |B| \text{ 且 } |B| \leqslant |C| \Rightarrow |A| \leqslant |C|.$$

推论 5.3.6 若 A 是无限集,则 $|\mathbf{N}| \leqslant |A|$.

这个推论表明,自然数集 $\mathbf{N}$ 是无限集中基数最小的.

定理 5.3.7 Zermelo 定理　设 A,B 是两集合,则 $|A| < |B|$, $|B| < |A|$, $|A| = |B|$ 三者中恰有一个成立.

定理 5.3.8 Cantor-Bernstein 定理　设 A,B 是两集合,若 $|A| \leqslant |B|$ 且 $|B| \leqslant |A|$,则 $|A| = |B|$.

定理 5.3.7 与定理 5.3.8 表明:基数与通常的实数一样具有线性序关系.

定理 5.3.9 Cantor 定理　设 A 为任意集合,则有 $|A| < |\mathscr{P}(A)|$.

利用定理 5.3.9,可以构造基数越来越大的集合;换言之,基数可按"大小"序构成的一个无限序列.

定理 5.3.10 设集合 A,B,C,A_1,A_2,B_1,B_2,则有

(1) $A_1 \sim B_1$ 且 $A_2 \sim B_2 \Rightarrow A_1 \times A_2 \sim B_1 \times B_2$;

(2) $A_1 \cap A_2 = \varnothing$ 且 $B_1 \cap B_2 = \varnothing$ 且 $A_1 \sim B_1$，$A_2 \sim B_2 \Rightarrow A_1 \cup A_2 \sim B_1 \cup B_2$；

(3) $A \sim B$ 且 $C \cap (A \cup B) = \varnothing \Rightarrow (A \cup C) \sim (B \cup C)$；

(4) $A \sim B \Rightarrow \mathscr{P}(A) \sim \mathscr{P}(B)$.

以下是有关可列集的若干重要性质.

定理 5.3.11 设 A, B 是可列集，则 $A \cup B$，$A \cap B$，$A \setminus B$，$A \dot{-} B$ 都是可列集.

定理 5.3.12 设 A, B 是可列集，则 $A \times B$ 是可列集.

定理 5.3.13 设 $|X| \geqslant \aleph_0$，则存在集合 X_1 满足：$X_1 \subset X$，且 $|X_1| = \aleph_0$ 且有 $(X \setminus X_1) \sim X$.

定理 5.3.14 自然数集 **N** 的全部有限数列的集合是可列集.

定理 5.3.15 下列集合均为可列集.

(1) **Q**.

(2) 代数数的全体是可列集（以有理数为系数的多项式的根，称为"代数数"）.

(3) **R** 中两两不相交的区间全体构成可列集.

(4) **R** 中连续函数的极值点的全体是可列集.

定理 5.3.16 **R** 中单调函数的不连续点的全体是可列集.

例 5.3.17 下列集合都是可列集.

(1) **R** 中端点是有理数的区间全体.

(2) $^2\mathbf{R}$ 中，中心及半径均为有理数的圆（周）的全体.

(3) $^3\mathbf{R}$ 中两两不相交的立方体的全体.

(4) 全部有限维的矩阵（其元素是有理数）的全体.

以下是关于基数$\aleph$的若干性质.

定理 5.3.18 设集合 A, B 的基数均为$\aleph$，则 $A \cup B$，$A \times B$ 的基数也是$\aleph$.

定理 5.3.19 设 $|A| = \aleph$，$|B| = \aleph$，则 $A \cup B$，$B \setminus A$，$B \dot{-} A$ 的基数都是$\aleph$.

例 5.3.20 下列集合的基数都是$\aleph$.

(1) $\mathbf{R}$, ${}^{n}\mathbf{R}(n\in\mathbf{N})$.

(2) $[0,1]\times[0,1]$.

(3) 超越数全体($\mathbf{R}$ 中除去代数数后所剩余的实数,称为超越数).

(4) ${}^{\mathbf{N}}\mathbf{N}$.

读者注意,我们常用${}^{A}B$ 表示由所有的映射 $f: A\to B$ 构成的集合. 有些文献中也记作 B^{A};特别当 $B=\{0,1\}$是含有两个元素的集合时,${}^{A}B$(或 B^{A})也记作${}^{A}2$(或 2^{A}).

例 5.3.21 Cantor 三分集的基数是$\aleph$.

它是由单位区间经过一系列删除过程得到的(参看图 5.1).

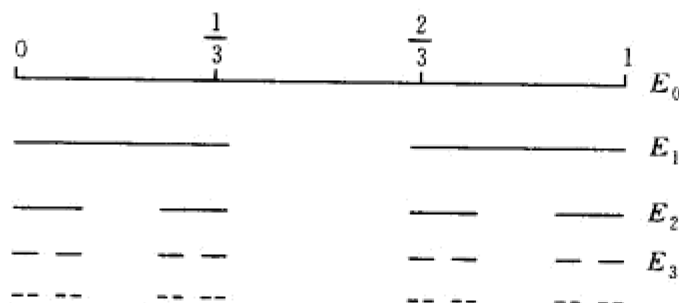


图 5.1

设 E_0 是区间$[0,1]$,E_1 是 E_0 中去掉开区间$\left(\frac{1}{3},\frac{2}{3}\right)$后得到的集合,所以 $E_1=\left[0,\frac{1}{3}\right]\cup\left[\frac{2}{3},1\right]$. E_2 是由 E_1 集合的每一个区间中,删去中间长度为$\frac{1}{3}$的开区间后得到的集合,所以

$$E_2=\left[0,\frac{1}{3^2}\right]\cup\left[\frac{2}{3^2},\frac{1}{3}\right]\cup\left[\frac{2}{3},\frac{7}{3^2}\right]\cup\left[\frac{8}{3^2},1\right].$$

一般而言:E_k 是从 E_{k-1}的每一个区间中去掉中间长度为 1/3 的

开区间后得到的集合. 因此,E_k 是由 2^k 个区间长度为 3^{-k}的闭区间组成. G. Cantor 构造的三分集是

$$F = \bigcap_{k=0}^{\infty} E_k.$$

换言之,F 是由所有 E_k 的“公共点”组成,即 F 是由$[0,1]$上三进制表示中不含数字“1”的小数组成,即所有小数具形式:

$$a_1 3^{-1} + a_2 3^{-2} + a_3 3^{-3} + \cdots.$$

其中 $a_i = 0$ 或 $a_i = 2$.

进一步而言,由于上述所有三进制小数(表示法中 a_i 含有数字“1”的)全体构成的集合,其基数是$\aleph_0$,因此 G. Cantor 三分集 F 的基数

$$|F| = \aleph.$$

注 Cantor 三分集是一个著名的“分形集合”,它的许多性质,在其他分形上均可看到:

(1) F 是自相似的. F 在区间$[0, 1/3]$和$[2/3, 1]$中的部分与 F 几何相似,相似系数为 1/3. F 在 E_2 中的部分与 F 相似,相似系数为 1/9,…集合 F 包含许多相似系数不同的相似子集.

(2) 集合 F 有“精细结构”,即在任意小的尺度内部包含整体特性.

(3) 集合 F 有复杂的构造.

(4) F 是由递归过程构造的.

(5) F 不容易用欧氏几何的术语来描述,它的点的轨迹不满足简单的几何条件,它也不是简单方程的解.

(6) 虽然 F 的基数是$\aleph$,但它不能用通常的度量,如长度来数量化. 在任何合理的长度定义下,其长度为零.

由例 5.3.20 可知,定义域是自然数集 **N**,值域也是自然数值 **N** 的所有可能的全函数构成的集$^{\mathbf{N}}\mathbf{N}$ 是不可列集. 可用 Cantor 对

角线法来证明. 设定义于 **N** 上的所有全函数 $f_i(i\in\mathbf{N})$,列表如下,它们所对应的函数值列于如下:

$$
\begin{array}{lllll}
f_1: & n_{11} & n_{12} & n_{13} & n_{14}\cdots \\
 & & \searrow & & \\
f_2: & n_{21} & n_{22} & n_{23} & n_{24}\cdots \\
 & & & \searrow & \\
f_3: & n_{31} & n_{32} & n_{33} & n_{34}\cdots \\
 & & & & \searrow \\
f_4: & n_{41} & n_{42} & n_{43} & n_{44}\cdots \\
 & \vdots & \vdots & \vdots & \vdots\ \searrow
\end{array}
$$

仿照 Cantor 的做法,构造一个新的函数 $f_*: n_{11}^*\ n_{22}^*\ n_{33}^*\ n_{44}^*\cdots$,使得 $n_{ii}^*\neq n_{ii}(i\in\mathbf{N})$. 从而可知 $f_*\in{}^{\mathbf{N}}\mathbf{N}$,但它不在上述表中. 因此 ${}^{\mathbf{N}}\mathbf{N}$ 是不可列集.

如前所述,可以被写出来使用的计算函数的程序集合是一个可列集(见例 5.2.7). 因此在自然数集合 **N** 上,就存在着不能用任何程序来计算的函数.

定理 5.3.22 对任意集合 A,有 ${}^{A}2\sim\mathscr{P}(A)$.

定理 5.3.23 设 A 是有限集,$|A|\geqslant 2$ 且 $|B|\geqslant\aleph$,则 ${}^{B}A\sim{}^{B}2$.

5.3.2 Cantor 猜想——连续统假设(CH)

由 Cantor 定理(定理 5.3.9)知,对于任意集合 A 有

$$|A|<|\mathscr{P}(A)|.$$

当 $A=\mathbf{N}$ 时,有

$$|\mathbf{N}|<|\mathscr{P}(\mathbf{N})|,$$

即

$$\aleph_0<2^{\aleph_0}=\aleph,$$

也就是

$$\aleph_0<\aleph.$$

在$\aleph_0$与$\aleph$之间还有没有其他的基数呢？这是Cantor早在一百多年前就提出的猜想：他认为不存在介于$\aleph_0$与$\aleph$之间的基数.这就是**连续统假设**. 1900年数学家Hilbert在巴黎数学家大会上提出的23个未解决的数学问题，向新世纪(即20世纪)数学家进行的挑战，其中第一个就是Cantor的连续统假设是否成立？这是一个在20世纪仍然未解决的问题.

目前的现状是，在公理集合论的框架内，得到如下的结论：1938年，Gödel证明了CH相对于集合论的其他公理是相容的(协调的). 经过25年后，1963年Cohen，P 证明了CH的否定对于其他公理也是相容的. 因此，可以说CH完全独立于集合论的其他公理. 所以凡承认Cantor连续统假设是正确的，在这种前提下研究的集合论称为**Cantor集合论**. 不承认上述假设正确的，称为**非Cantor集合论**.

就目前的发展来看，公理集合论的理论体系并不完善. 而“集合论是全部数学理论的基础”也有种种不同的含义. 事实表明，集合论仍是一个发展中的理论.



6 集合论悖论与公理集合论

由于集合中的元素可以是各种各样的客体,集合概念的引入,急剧地扩大了数学研究的视野. 比如符号、文字、声音、图形、图像以致于光、电、热等,原则上均可视为集合中的元素. 在如此广泛的概念下,难免会产生种种悖论. 这种情况 Cantor 本人也早有觉察. 为了消除这些悖论,对集合的概念,必须加以限制,从而产生公理集合论.

首先介绍悖论,然后再谈公理集合论.

6.1 悖论

按照悖论出现的年代叙述如下.

6.1.1 Burali-Forti 悖论(最大序数悖论)

这个悖论 Cantor 在 1895 年就已知道,但未发表,1897 年被意大利数学家 Burali-Forti 再次发现并发表.

设集合 Ω 由所有序数组成,是一个良序集,它的序数为 λ. 根据序数理论,Ω 中任何元素 α 均小于 λ, 因此 $\lambda \notin \Omega$. 另一方面,由 Ω 的定义知 $\lambda \in \Omega$, 从而产生矛盾.

6.1.2 Cantor 悖论(最大基数悖论)

该悖论 1899 年发现,1932 年发表.

设集合 S 是由所有集合组成(即 S 是所有集合的集合),$\mathscr{P}(S)$ 是 S 的幂集,它们的基数分别是 $|S|$, $|\mathscr{P}(S)|$. 现在问 $|S| >$

$|\mathscr{P}(S)|$,还是$|S|<|\mathscr{P}(S)|$?

一方面,由集合论中的 Cantor 定理(见定理 5.3.9)有$|S|<|\mathscr{P}(S)|$. 另一方面,由于 S 是所有集合的集合,是集合中最大者,所以有 $S\supset\mathscr{P}(S)$. 于是有$|S|>|\mathscr{P}(S)|$. 因此,$|S|>|\mathscr{P}(S)|$, $|S|<|\mathscr{P}(S)|$同时成立,导致矛盾.

6.1.3 Russell 悖论

这个悖论于 1902 年提出,同时也被 Zermelo 独立发现.

构造一集合 S: $S=\{x|x\notin x\}$.

换言之,S 是由满足条件"$x\notin x$"的那些元素组成的集合,现在问 S 是否是它自己的元素? 即,$S\in S$ 还是 $S\notin S$?

若 $S\notin S$, 由于 S 是由所有满足条件 $x\notin x$ 的集合所组成,现在 $S\notin S$, 可知 S 应当在集合 S 中,即 $S\in S$. 反之,若 $S\in S$, 由于 S 中的元素均有性质 $x\notin x$, 所以对 S 而言也应有 $S\notin S$. 这就是著名的 Russell 悖论. 由于这个悖论涉及的概念极少,所以极其重要.

为了加深理解,再从另外的角度阐明如下.

Russell 指出,全部集合可以明确地划分为两类:一类是包含自身作为元素的集合(称为异常集);另一类是不包含自身作为元素的集合(称为正常集). 例如:包含全体多于 3 个元素的集合组成的集合是它自身的一个元素,因为含有多于 3 个元素的集合也不止 3 个. 包含全体"概念"(以"概念"为元素)所组成的集合,也是它自身的一个元素,这些都是异常集的例子. 而正常集则更是比比皆是,例如由所有桌子组成的集合,它本身当然不是桌子. 所有猫组成的集合,它本身当然不是猫!

现在构作一个集合如下:

$$W=\{x\mid x\text{ 是正常集}\}.$$

换言之,W 是由所有正常集构成的集合.

问 W 是怎样的集合？

若 $W \in W$，则根据 W 的定义，W 是正常集，而所有正常集都不是自身的元素，所以 $W \notin W$. 反之，若 $W \notin W$，则可知 W 是异常集，根据定义所有异常集都有性质 $W \in W$. 所以，不论 W 是哪一种集合，矛盾总会发生.

6.1.4 Richard 悖论

法国数学家 Richard 1905 年提出下述悖论，1906 年 Dixon 也发现这个悖论. 这是一个关于有限可定义性的悖论（对于程序理论极为重要!）.

任意法语句子总是由 26 个法语字母、逗点和字母间的空格构成的有穷长的符号串. 设由能用有穷个字加以定义的一切无穷十进位小数(例如“圆周率的小数部分”0.1415926535…)组成集合 $\mathscr{E}$. 显然 $|\mathscr{E}| \leqslant \aleph_0$，令定义出的全体小数按字典序排列为 E_1，E_2，…，E_n，… 其中

$$E_n = 0.x_{n1}x_{n2}\cdots x_{nn}\cdots$$

另外，利用 Cantor 对角线法构造一个无穷十进位小数 E^*，它定义为：“如果 $\mathscr{E}$ 中第 n 个小数 E_n 的小数部分的第 n 位数 $x_{nn} \neq 9$，则令 $x_{nn}^* = x_{nn} + 1$，若 $x_{nn} = 9$，则令 $x_{nn}^* = 0$”. 因此 E^* 是能用有穷个字定义的十进位小数，所以 $E^* \in \mathscr{E}$. 另一方面，由 E^* 的表达式又知 E^* 与 $\mathscr{E}$ 中任何一个小数都不相同，所以 $E^* \notin \mathscr{E}$. 产生矛盾.

6.1.5 Berry 悖论

这个悖论是 20 世纪初由 G. G. Berry 提出，1906 年由 Russell 加以研究. 这也是一个关于有限可定义性的悖论.

考虑下述命题：r 是“不能够用少于二十二个字来命名的最小的自然数”. 依照 r 的定义，r 是不能够用少于二十二个字而确定的. 然而该命题本身，却只用了二十一个字就确定了自然数 r.

6.1.6 Grelling 悖论

这个悖论于 1908 年提出，是由“自谓的(predicable)”与“非自谓的(nonpredicable)”概念所引起的. 所谓“自谓的”是指它的含义适用于自己，例如“抽象”的概念是抽象的，所以它是自谓的. 所谓“非自谓的”是指它的含义不适用于自己，例如“具体”的概念仍是抽象的而非具体的，所以它是“非自谓的”. 现在问“非自谓的”概念是哪一种？

如果“非自谓的”概念是自谓的，那么它适用于自己，所以它又是非自谓的. 如果“非自谓的”概念是非自谓的，那么它不适用自己，所以它又是自谓的. 无论是哪一种情况，均导致矛盾.

6.1.7 理发师悖论

这个悖论于 1919 年提出，是 Russell 悖论(见 6.1.3 节)的通俗化，叙述如下.

某个村庄的一个理发师，他只给村中所有不给自己理发的人理发，那么他是否应该给他自己理发?

具体地说，把村里的人分成两类，第一类是自己给自己理发的人；第二类是自己不给自己理发的人. 凡是自己给自己理发的人，理发师就不给他理发，凡是自己不给自己理发的人，理发师就应该给他理发. 现在问理发师该不该给自己理发？如果理发师自己给自己理发，这时理发师是第一类人，那么他就不应该给他自己理发，于是他又应该是第二类人. 如果理发师自己不给自己理发，这时理发师是第二类人，那么他就该给他自己理发，于是他又应该是第一类人. 总之，理发师既不能是第一类人，也不能是第二类人. 导致矛盾.

Russell 还指出他的悖论，既可以用集合论的语言来陈述，也可以用逻辑的语言来陈述. 关于 Russell 悖论，还有种种不同的

表述.

6.1.8 Minimanoff 悖论

该悖论于 1917 年提出.

集合 x_0 满足下列条件时,称为无底集:对于 x_0,存在集合列 $\{x_n\}$满足:

$$\cdots x_{n+1} \in x_n \in x_{n-1} \in \cdots \in x_1 \in x_0.$$

显然,若 x_0 是无底集,则$\{x_n\}$中的任何一个 x_n 也是无底集. 称不是无底集的集合为有底集. 构造集合 X:

$$X = \{\text{所有有底集}\},$$

问 X 本身是哪一种集?

若 X 是无底集,则有集合列$\{x_n\}$使得

$$\cdots x_{n+1} \in x_n \in x_{n-1} \in \cdots \in x_2 \in x_1 \in x_0 \in X.$$

于是 x_0 也是无底集,然而 $x_0 \in X$, 而 $X=\{\text{所有有底集}\}$,所以 x_0 又是有底集,产生矛盾. 反之,若 X 是有底集,则存在集合列:

$$\cdots X \in X \in \cdots \in X,$$

因此 X 又是无底集. 换言之,X 是有底集,又是无底集,产生矛盾.

6.2 公理集合论

一般认为上述悖论与 Cantor 朴素集合论中的一个重要的造集方法——概括原则:对于任意给出的性质,必定存在集合 S,它的元素恰好就是具有该性质的那些对象——过于广泛有关.

为了解决悖论,产生许多公理集合论,比较有名的是 ZFC 系统(Zermelo-Fraenkel-Cohen)与 GBN 系统(Gödel-Bernays-von Neumann).

6.2.1 ZFC 系统

下面列出该系统的公理并加以解释.

(1) **外延公理**(axiom of extensionality)

若集合 X 与 Y 含有相同的元素,则它们相等(即 $X=Y$). 换言之,一个集合完全由它的元素所决定.

(2) **空集存在公理**(axiom of the empty set)

存在着一个不含任何元素的集合$\varnothing$.

根据外延公理$\varnothing$是唯一的.

(3) **配对公理**(axiom of pairs)

任给两集合 X,Y 存在着仅含 X,Y 为元素的集合 Z. 例如,设 $X=\{1,2\}$,$Y=\{3,4\}$,则 $Z=\{\{1,2\},\{3,4\}\}$. (注意: $Z\neq\{1,2,3,4\}$!)

(4) **并集公理**(axiom of union)

设 A 是一个集合族,则存在着集合 S 使得 x 是 S 的元素当且仅当 x 是族 A 中某一个集合 X 的元素. 换言之,对任意给定的集合族 A,可以把 A 中元素 X(X 也是集合)里的元素 x 汇集到一起,组成一个新的集合 S. 例如 $A=\{X,Y\}$时 $S=X\cup Y$.

(5) **幂集公理**(axiom of power sets)

对于任意集合 A,$\mathscr{P}(A)$也是集合,它恰由集合 A 的全体子集构成.

(6) **无穷公理**(axiom of infinity)

存在着集合族 A 满足

1) $\varnothing\in A$;

2) 对于任意的集合 $X\in A$,存在集合 $Y\in A$ 使得集合 Y 恰含集合 X 中所有元素以及集合 X 自身. 换言之,存在一个集合 A,它含有无穷多个元素.

(7) **关于公式 Φ 的替换公理**(axiom of replacement for the

formula Φ)

若对于任意的 x 恰好存在唯一的 y 使得公式 $\Phi(x,y)$ 成立，则对于任意的集合 A，存在集合 B，它恰含元素 y 使得对某个 $x\in A$，公式 $\Phi(x,y)$ 成立. 换言之，由公式 $\Phi(x,y)$ 所定义的"有序对"的类的定义域包含在 A 中时，那么它的值域可以限制在集合 B 中.

特别，当公式 Φ 仅含一个变元时，即 $\Phi(x,y)$ 变成 $\Phi(x)$ 时，则有关于公式 $\Phi(x)$ 的子集公理：对于任意集合 A，存在着 B，它恰含集合 A 中满足公式 $\Phi(x)$ 的元素.

(8) **正则公理**(axiom of regularity)

任意非空集合必有一个 ϵ 极小元. 换言之，对于任意非空集 $X\neq\varnothing$，则必有一集合 Y，$Y\in X$，而任何集合 $Z\in Y$，则 $Z\notin X$.

正则公理表明一集合的元素都具有某种最小性质. 集合和它的元素具有层次关系. 因此，这一公理也叫基础公理或限制公理.

(9) **选择公理**(axiom of choice)

对于任意两两互不相交的非空集合族 A，存在一个集合 B，它与 A 中的每一个集合恰有一个公共元素.

由上述公理(1)～(8)构成的系统，称作 ZF 公理系统；由公理(1)～(9)构成的系统，称作 ZFC 公理系统.

为了加深理解，下面给出这些公理提出的背景，供学习参考.

6.2.2 注记

(1) 这些公理中的 2～7 都是对概括原则的某种限制(概括原则：任意给定一个性质 $P(\cdot)$，则存在着一个集合，它的元素恰好是具有性质 $P(\cdot)$ 的对象，即 $S=\{x\mid P(x)\}$. 这个原则在朴素集合论中经常采用. 从公理集合论的角度来看，它应该加以适当的限制，比如说：$P(x)=x\notin x$，或 $P(x)=x\in x$ 都是不允许的！这个原则最早由 Cantor 提出，沿用至今). 试图用这六条公理，把概

括原则中那些对集合运算，集合存在性等合理的内容保留下来，舍去那些导致悖论的性质.

(2) 这些公理中的公理1与公理8是对集合的具体描述. 例如外延公理说：一个集合由它的元素唯一决定. 一组元素决定一个集合，而不是多个集合. 例如元素"0,1,2,#"只能决定一个集合，因此

$$\{0,1,2,\#\} = \{\#,1,0,2\} = \{1,2,\#,0\} = \cdots$$

它们与集合中元素的次序无关!

由正则公理说明集合和它的元素具有某种层次关系，这样就排除了具有 $x \in x$(及 $x \notin x$)这种性质的集合.

(3) 关于公式 Φ 的替换公理与关于公式 Φ 的子集公理都是公理"模式"(schema)，它们都有无限多条. 因此，ZF/ZFC 集合论不是有穷公理化的理论，而是递归公理化的理论.

(4) 关于 Φ 的子集公理模式，在1908年 Zermelo 给出的公理中是没有的，他只是列举出子集合公理，当时对于"什么是性质"也未能说清楚. 这个公理模式和概括原则的不同点在于：它断言，构成新集合 B 的元素仅仅是集合 A 中满足公式 Φ 的元素. 换言之，不是满足任意性质的元素都能决定一个集合，而首先是这些元素已经含在某一个集合中了. 而且，也不是任何一个集合的任何一部分元素都能构成一个集合，它还要满足某种性质(这个性质通过公式 Φ 表示出来)后才能构成一个集合.

(5) 替换公理是独立于其他公理的，有些重要的集合，只有通过替换公理才能获得.

(6) 关于选择公理，在所有的公理中，它是唯一只涉及到"存在"性的公理. 一般而言(尤其是无穷集)，对于任意一个集合族如何从中"选择"元素来构成新的集合，没有给出任何"构造性"的方法. 因此许多数学家对这条公理产生极大的怀疑，承认与反对者都有. 但这条公理是很深刻的，它接触到了数学的本质.

关于选择公理还要说明如下：

1）在选择公理明确提出之前，有些数学家在证明某些定理时（选择公理是 1890 年数学家 Peano 在证明常微分方程解的存在性时，首次明确地陈述它．1904 年 Zermelo 在证明良序定理时又使用了它），已经使用了它，只是"不自觉"而已．

2）迄今为止，已经证明在数学的各个领域中，有许多重要的定理与选择公理是等价的．

① Zorn lemma（分析数学）：若 A 是一个集族使得 A 中的任意链（chain）B 的并仍在 A 中，则 A 中必含有一个$\subseteq$-极大集[①]．

② Kurepa 原理（集合论）：对于任意的集合族，存在着$\subseteq$-极大子族 F 使得在 F 上有一个二元关系 S 具有下列性质：对于任意的 $A,B\in F$，有关系 S 如下：

(i) 集合 A,B 重合，即 $A=B$（见图 6.1(a)）．

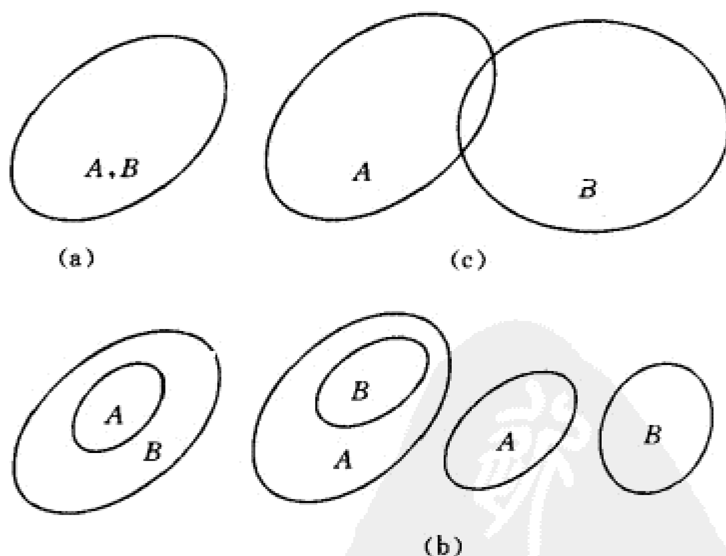


图 6.1

① 注，指在集合包含关系下的极大集．

(ii) $A\setminus B=\varnothing$或$B\setminus A=\varnothing$或$A\cap B=\varnothing$(见图 6.1(b)).

(iii) $A\not\subseteq B$ 且 $B\not\subseteq A$ 且 $A\cap B\neq\varnothing$(见图 6.1(c)).

上述原理是明显的,它说明无论怎样的集族,其中任意两集合间的可能关系总是这样的. 这种情况与日常的经验是完全相符的.

③ 基数三歧性(trichotomy of cardinals)(集合论):设 M,N 为基数(有限或无穷),则有

(i) $M<N$ 或

(ii) $M=N$ 或

(iii) $M>N$.

④ 良序原理(well-ordering theorem)(集合论):任意集合均可良序化.

⑤ 极大理想定理(greatest ideal theorem)(代数学):对于任意有单位元的且至少含有另一元素(不同于单位元)的格,必有一个极大理想.

⑥ 设 $V(A)$是一个向量空间,则它的生成集 A 含有 $V(A)$的基底(basis)(线性代数学).

⑦ Downward Löwenheim-Skolem 定理(数理逻辑):任意无穷的一阶语句集 A 的模型必有一个子模型,它的基数不大于 A 的基数.

⑧ Tychonoff compacteness 定理(拓扑学):任何紧致拓扑空间的积空间仍是紧致空间.

3) 选择公理(AC)在 ZF 集合论中是不可判定的. 换言之,如果 ZF 是相容的,则系统 ZF+AC=ZFC 也是相容的;并且系统 ZF+¬ AC(¬ AC 表示选择公理不成立)也是相容的.

但是 ZF 系统是不是相容的呢? 很多数学家认为它是相容的,然而迄今还没有严格的数学证明.

6.2.3 GBN 系统

这种集合论中，包含两种不同的对象：集合（set）与类（class）. 公理如下.

A. 1 **外延性**（extensionality）：若类 X 与 Y 含有相同的元素，则 $X=Y$.

2 集合都是类（但类未必是集合）.

3 若 $X\in Y$，则 X 是集合.

4 对任意的集合 X,Y 存在集合 $\{X,Y\}$.

B **概括原则**（comprehension）：设 φ 是任意公式，其中不含类的变量，则对任意两集 X,Y 存在集合 $Z=\{x\mid\varphi(x,X,Y)\text{成立}\}$.

C. 1 **无穷性**（infinity）：存在无穷集.

2 对于任意集 X，存在集合 $\bigcup X$.

3 对于任意集 X，存在幂集合 $\mathscr{P}(X)$.

4 替换公理（replacement）：设类 F 是一个函数，X 是一个集合，则 $F(X)$ 是集合.

D **正则公理**（regularity）（与 ZF 系统同）.

E **选择公理**（choice）：存在选择函数 F 使得对于任意非空集合 X 有：$F(X)\in X$.

从表面看，GBN 系统包含了 ZFC 系统（因为可以证明凡是集合论命题在 ZFC 中可证，则必在 GBN 中可证）. 然而我们也有结论：凡是集合论命题，如果其中仅仅含有集合变元（不含类变元）在 GBN 中可证，则必在 ZFC 中可证. 所以就集合论命题而言，两种系统是一样的.

组合学与图论

7 若干著名的组合学和图论问题

7.1 幻方与中国古代的传说

把 n^2 个数：1，2，…，n^2 排成 $n\times n$ 的阵列，使每行中的数之和、每列中的数之和、两对角线上的数之和都等于同一个整数 S，称此阵列为一个 n 阶**幻方**（magic square）. 例如下面是一个 3 阶幻方和 4 阶幻方：

$$\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} \qquad \begin{bmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{bmatrix}$$

已经证明，除 2 以外的正整数 n，都可构造 n 阶幻方.

幻方最早出现在中国古代的一本用于占卜的书"易经"（公元前 2200 年）中，其中描述了两个图. 一个图称为"洛书"，传说是出现在从洛河浮现的神龟背上. 如图 7.1.

它实际上是如下的一个阵列：

$$\begin{matrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{matrix}$$

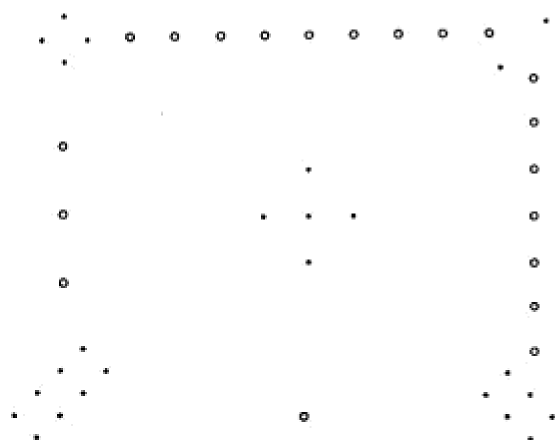


图 7.1

它是一个 3 阶幻方.

另一个图称为“河图”,传说是出现在从后河(现今的黄河)跃出的龙马背上.

它实际上是以下形式的一个阵列:

			7			
			2			
		10		10		
8	3		5		4	9
		10		10		
			1			
			6			

这个阵列也具有一定的规律性:内层相邻的数之和等于外层的数之和等等.例如:$5+3=8$,$5+1=6$,等等;$3+10+2=8+7$,$3+10+1=8+6$,等等.

幻方的定义还可推广如下:一个 n 阶非负整数阵列,每行、每列及两对角线上元素之和都相等,则称此阵列为一个 n 阶幻方.如要求 n^2 个数彼此不同,则称它为**异元幻方**.如要求 n^2 个数是连

续的非负整数,则称它为**连元幻方**. 如要求 n^2 个元素为 1,2,…,n^2,则称它是一个**始元幻方**. 前面所说的幻方即为始元幻方.

最近国内有一些人做出了各种形状的幻方,如棱形幻方,圆形幻方等.

7.2 36 军官问题和拉丁方

Euler(欧拉)曾提出以下问题:有 36 名军官,分别来自 6 个不同的团,每个团的 6 名军官又具有 6 种不同的军衔. 能否把他们排成 6×6 的阵列,使每行每列的 6 名军官恰好来自 6 个不同的团且有 6 种不同的军衔.

把 6 个团用 1 到 6 的整数来表示,并令 $S=\{1,2,3,4,5,6\}$. 如果能把这 6 个数排一个 6×6 的阵列 A,且使每行每列恰含这 6 个数,这个方阵就是一个**拉丁方**(Latin square). 36 个军官的排列方法应使他们的团的番号对应这个拉丁方 A.

同样,把 6 个军衔也用 S 中的元素来表示,也把这 6 个数排成一个 6×6 的方阵 B,且使每行每列恰含这 6 个数,得到另一个拉丁方. 36 个军官的排列方法应使他们的军衔对应拉丁方 B.

又由于每一名军官在 6×6 方阵中只能出现一次,如果用(a_i, b_j)表示一个来自第 a_i 团军衔为 b_j 的军官,则全部 36 名军官所对应的二元数组的集合应为

$$\{(a_i,b_j) \mid i,j=1,2,\cdots,6\} = S\times S. \qquad (7.1)$$

这就是说 A 与 B 这两个拉丁方不是任意的,它们必须满足条件(7.1).

于是,36 军官问题就转换成是否存在两个满足条件(7.1)的 6 阶拉丁方问题. 已经证明,不存在这样的两个拉丁方,所以 36 军官问题的答案是否定的. 详见定理 13.2.2.

7.3 Königsberg 7 桥问题与中国邮递员问题

Königsberg(哥尼斯堡)是俄罗斯的一个城市，在苏联时期曾称为加里宁格勒. 市内有一条河，河中有两个岛，在两岸与岛之间有七座桥，如图 7.2. 居民们经常在此散步，人们自然而然提出了这样一个问题：如果从某一处出发，能否经过每座桥恰一次，又回到出发点.

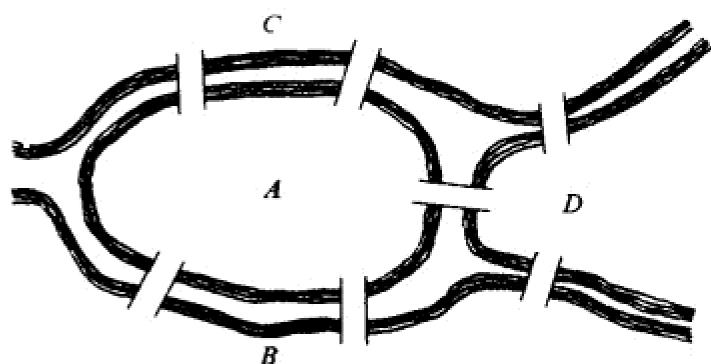


图 7.2

据传有人写信请教当时的大数学家 Euler，他用图论方法解决了该问题.

为了解决此问题，可把每一块陆地用一个点表示，两岸与岛分别用 A,B,C,D 这 4 个点表示，用点之间一条边表示桥，于是得到了一个图(图 7.3). 问题就化为在此图中找一条路线，从某一点出发，经过每一条边恰好一次，又回到出发点，这就是所谓**欧拉闭迹问题**.

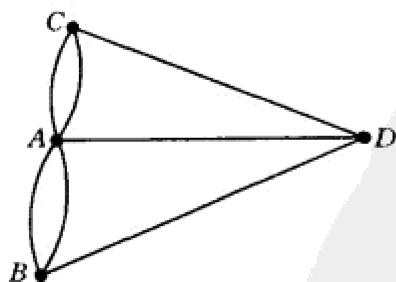


图 7.3

1962 年中国数学家管梅谷推广了欧拉闭迹问题，提出邮递

员问题，被国际学术界称为**中国邮递员问题**(Chinese postman problem). 问题的提法为：一个邮递员在一个街区内送信，从某一点出发，经过每一条街道，又回到出发点，如何设计一个投递路线，使总路程最少. 该问题用图论的术语表达就是在一个有边权的图中找一个总权最小的闭通道.

7.4 鸽子笼原理与 Ramsey 数

所谓鸽子笼原理，是说 $n+1$ 只鸽子飞入 n 个笼子. 则至少有一个笼子里有两只以上的鸽子. 这是一个非常浅显的原理，也很易用反证法给出一个简捷的证明. 鸽子笼原理又称为抽屉原理、邮箱原理等.

把鸽子笼原理推广一下，可以得到以下的推广的鸽子笼原理：设 $q_1, q_2, \cdots, q_n$ 为 n 个正整数，若有 $q_1+q_2+\cdots+q_n-n+1$ 只鸽子飞入 n 个笼子，则或者第 1 个笼子里至少有 q_1 只鸽子，或第 2 个笼子里至少有 q_2 只鸽子，…，或第 n 个笼子里至少有 q_n 只鸽子.

简单鸽子笼原理正是推广的鸽子笼原理 $q_1=q_2=\cdots=q_n=2$ 时的特殊情形.

1924 年英国逻辑学家 Ramsey 进一步推广了鸽子笼原理，得到 Ramsey 定理和著名的 Ramsey 数，详见 8.17 节.

7.5 地图着色与四色猜想(定理)

通常在绘制地图时，相邻的国家着不同的颜色. 逐渐地，人们发现，任何一张地图，用 4 种颜色就足够了，这是否是一个一般性的规律呢？据记载，正式提出此问题大约是在 19 世纪中叶，用图论术语可表达如下：设一个平面地图中每个国家是由一个单连通

域构成，两个国家相邻指它们有一段公共边界线．我们用点代表国家，两个国家相邻则对应的两个点之间用边相连，于是得到一个平面图．**四色猜想**(four color conjecture)就成为：每一个平面图，可用 4 种颜色对其顶点着色，使相邻的点着不同的颜色．

这个猜想吸引了许多学者，许多人都曾经宣布证明了此猜想，但后来都被发现证明中有错．1976 年，美国的三位科学家 K. Appel，W. Haken 和 J. Koch 用计算机作出了一个证明．据说在计算机上运行了上千小时．虽然他们的证明通过了权威的审查，但仍有人心中存疑，谁能担保程序在上千小时的运行过程中一点错都不出？不少人仍相信传统的手工证明方法．详见 11.6.4 节．

7.6　绕行世界与旅行商问题

英国数学家 Hamilton 爵士于 1859 年设计了一种游戏：用一个正 12 面体的 20 个顶点代表世界上 20 个大城市，要求游戏者从某个城市出发，沿边经过每个城市恰一次，又回到出发点．虽然由于这个游戏的乏味，使购买这个设计的玩具商并未因此发财，但这个游戏中蕴含的数学原理却使数学家们着迷了一百多年，至今仍是一个热门课题．

如果把一个正 12 面体画成一个图，如图 7.4，问题就是：在这个图中找一条经过每个点恰一次的闭回路，称为哈密尔顿圈．图的哈密尔顿问题，指的就是研究图中存在哈密尔顿圈的条件．该问题是图论中的核心问题之一，对于推动图论的发展起了很大的作用，已得到许多成果，而且新的结果还在不断出现．

后来，此问题又发展成为以下的最优化问题：用一个赋权完全图表示一些城市之间的交通图，顶点代表城市，边的权代表城市之间的距离或旅行费用．一个旅行推销员从一个城市出发，经过每个城市恰一次，又回到出发点，应如何选择旅行路线，使总权最

小. 这就是所谓旅行商问题(travelling salesman problem). 如果用穷举法来进行计算,对于一个完全图来说,需要进行$\frac{1}{2}(n-1)!$个哈密尔顿圈的计算,其计算量随 n 的增大而急剧增加,发生所谓的“组合爆炸”而使最先进的计算机都无能为力. 因此必须寻找一种好的计算方法,使其计算量是 n 的多项式函数. 对旅行商问题,至今仍未找到这样的算法. 旅行商问题的研究还推动了算法理论的发展.

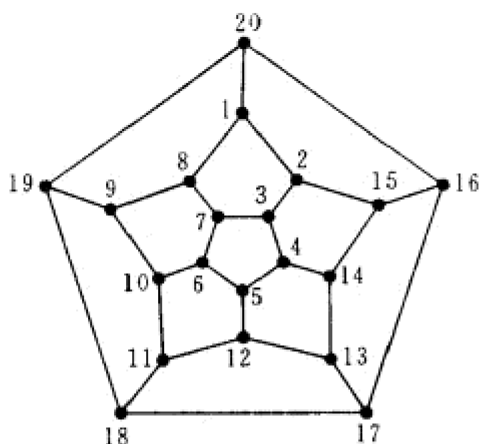


图 7.4

7.7 电路与网络

电路是图的一个直接实际背景. 把电路的节点对应图的顶点,电路的每个支路及支路上的元件对应图的边,这样就得到一个图. 要解这个电路,要用分支回路来建立一个线性方程组. Kirchhoff(基尔霍夫)利用图论中树的理论来研究电路,他证明了为解这个电路并不需要考虑这个图中的每一个回路,而只要考虑这个图的一个生成树,对由这个生成树所决定的独立圈建立方程就行了.

图论可应用于更加广泛的网络问题,例如运输网络或交通网络的最大流问题;通信网或输电网的连通性与可靠性问题;最近兴起的全球高速信息公路及局部计算机网都需要利用图论和组合学.

7.8 从分子结构到图的计数

大概是 Cayley(凯莱)最早(1857 年)将图论应用于化学领域. 他在研究同分异构体的数目时,用图论方法将问题转化为计算树的数目的问题. 例如给定了碳原子的数目 n,可形成多少种饱和碳氢化合物 C_nH_{2n+2}? 转化为图论问题,就是求 n 个点的树的数目,其中每个点的度为 1 或 4.

把同分异构体问题稍稍推广一下,如果给定了分子结构的形式,结合不同的原子,能形成多少种化合物? 例如,在一个苯环上结合 H 原子,或 OH,或 CH_3,可形成多少种化合物. 还可进一步研究由多个苯环构成的六角形结构问题.

撇开实际背景,可以研究抽象的图的数目,特别是不同构的图的数目. 这方面 Pólya(波利亚)做出了重要的贡献,他将群论应用于组合计数问题,著名的 Pólya 定理给出了计算不同构图数目的一般公式. 但是具体计算某类图的数目时,为了得到简洁的公式,仍然遇到了很多困难,许多类图的计数问题解决了,但仍然有更多类图的计数问题还未解决. 见 9.11 节.

7.9 Kirkman 女生问题与三元系

Kirkman(科克曼)是一位 19 世纪的英国数学家,19 世纪中叶,在英国数学家中掀起了一股不小的组合数学研究热潮,Hamilton,Cayley 都在其中. Kirkman 于 1850 年在名为《女士与先生之日记》的杂志上发表文章,提出以下的所谓**科克曼女生问题**(Kirkman's schoolgirl problem):一位女教师每天带领她班上的 15 名女生去散步,她把女生每天 3 人一组分成 5 组,问能否作出一个连续 7 天的分组方案,使任何两个女生在这 7 天中恰有一次

分在同一个组里.

首先可以初看一下这个问题的合理性：由于任何两人在 7 天内恰有一次分在同组，因而 7 天的分组集合中应含有 $\binom{15}{2}=105$ 个二元子集. 另一方面 7 天共 35 组，每一组含有 3 个二元子集，总共含有二元子集数也是 105(35×3). 因而初看问题提法是合理的，剩下的是如何排出散步方案. Kirkman 给出了一个方案，见 13.4 节.

可以把女生问题推广如下：设 X 是一个 v 元集合，是否存在 X 的三元子集簇：$X_1,X_2,\cdots,X_b$，使 X 的任意两个元素同时出现在某个子集 X_i 中恰一次(或称相遇恰一次). 这就是所谓 Steiner(斯坦纳)三元系问题，详见 13.4.5 节.

7.10 试验设计与组合设计

试验是科学研究与生产实践的基本手段，为了节省开支、减少成本，必须做尽量少的试验而取得较满意的结果. 试验设计正是研究如何减少试验次数的方法. 下面的配方问题是试验设计的典型问题.

配方问题：假设用 4 种原料配制一种饮料，而每一种原料又有 n 种浓度，怎样设计一个试验方案，求得最佳的配方，且试验次数尽可能少.

用 $A_i,B_i,C_i,D_i(i=1,2\cdots,n)$ 表示这 4 种原料的浓度，每一个配方可用数组 (A_i,B_j,C_k,D_l) 表示，因而全部配方个数为 n^4，当 n 较大时，试验次数太多. 现在把每一个配方想象为一个超立方体中的格子点. 如果只取其中某些有代表性的点，且在立方体中的分布具有一定的均匀性，那么在这些点上所作的试验结果就可反映整个立方体上的情况，从而得到近似的最佳方案. 因此，试验设

计是一种寻求最佳方案的近似方法.

最常用的试验设计方法为**正交试验设计法**,它的最基本的工具是正交拉丁方,能把试验次数从 n^k 降到 n^2,因而当因素数(指配方原料数)较多时,次数的减少是显著的. 近年来,我国学者王元、方开泰提出一种基于数论方法的**均匀设计法**,可把试验次数从 n^k 降至 n.

把试验设计抽象成为对一个有限集合 X 作出子集簇 B_1, B_2,…,B_b 满足一定的均匀性条件,例如,每个子集的元素个数相同,每个元素在子集簇中出现的次数相同,每两个元素同时出现在子集簇中的次数相同,等等. 这就是组合设计一般研究的问题. 详见第 13 章.



8 组合公式和组合数

8.1 二项式系数的基本恒等式

定义 8.1.1 以下形式的数称为**二项式系数**(binomial coefficient):

$$\binom{r}{k}=\frac{r(r-1)\cdots(r-k+1)}{k!},r\text{ 为实数},k\text{ 为非负整数}.$$

公式 8.1.2 二项式系数有以下恒等式:

(1) $\binom{n}{k}=\binom{n}{n-k}$,$k,n$ 为非负整数且 $k<n$.

(2) 杨辉三角形公式或 Pascal 公式:

$$\binom{r}{k}=\binom{r-1}{k}+\binom{r-1}{k-1}.$$

(3) $\binom{r}{k}=\frac{r}{k}\binom{r-1}{k-1}$.

(4) $\binom{-r}{k}=(-1)^k\binom{r+k-1}{k}$.

(5) $\binom{r}{m}\binom{m}{k}=\binom{r}{k}\binom{r-k}{m-k}$,$m,k$ 为非负整数.

(6) $\sum\limits_{k=0}^{n}\binom{r+k}{k}=\binom{r+n+1}{n}$.

(7) $\sum\limits_{k=0}^{n}\binom{k}{m}=\binom{n+1}{m+1}$,$m,n$ 为非负整数.

8.2 二项式定理及有关和式

定理 8.2.1 二项式定理(binomial theorem)：

$$(1+z)^n = \sum_{k=0}^{n} \binom{n}{k} z^k;$$

$$(1+z)^x = \sum_{k=0}^{\infty} \binom{x}{k} z^k,$$

x, z 为任意复数且 $|z| < 1$.

公式 8.2.2 有以下与二项式定理有关的和式：

(1) $$\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k+1}\binom{n}{k} = \frac{n}{n+1},$$

$$\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k}\binom{n}{k} = \sum_{k=1}^{n} \frac{1}{k}.$$

(2) $$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0,$$

$$\sum_{k=0}^{\infty} (-1)^k \binom{x}{k} = 0, \quad x \text{ 为复数且 } R(x) > 0.$$

(3) $$\sum_{k=a}^{\infty} (-1)^k \binom{x}{k} = (-1)^a \binom{x-1}{a-1} + (-1)^n \binom{x-1}{n}.$$

(4) $$\sum_{k=0}^{n} \frac{(-1)^k}{\binom{x}{k}} = \frac{x+1}{x+2}\left[1 + \frac{(-1)^n}{\binom{x+1}{n+1}}\right].$$

(5) $$\sum_{k=0}^{n} \frac{1}{\binom{x+k}{k}} = \frac{x}{x-1}\left[1 - \frac{1}{\binom{x+n}{n+1}}\right].$$

8.3 二阶组合恒等式

和式中含有两个二项式系数的等式称之为**二阶恒等式**.

(1) $\sum_{k=0}^{n}\binom{x}{k}\binom{y}{n-k}=\binom{x+y}{n}$, x,y 为复数.

(2) $\sum_{k=r}^{n-s}\binom{k}{r}\binom{n-k}{s}=\binom{n+1}{r+s+1}$, r,s 为非负整数.

(3) $\sum_{k=1}^{n}k\binom{n}{k}^2=\frac{(2n-1)!}{[(n-1)!]^2}$.

(4) $\sum_{k=j}^{n}\frac{\binom{z}{k}}{\binom{x}{k}}=\frac{x+1}{x-z+1}\left[\frac{\binom{z}{j}}{\binom{x+1}{j}}-\frac{\binom{z}{n+1}}{\binom{z+1}{n+1}}\right]$.

(5) $\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{1}{\binom{b+k}{c}}=\frac{c}{n+c}\frac{1}{\binom{n+b}{b-c}}$, b,c 为整数且 $b\geqslant c>0$.

(6) $\sum_{k=1}^{\infty}\frac{1}{k^2\binom{k+n}{k}^2}=\binom{2n}{n}\left[\frac{\pi^2}{6}-3\sum_{k=1}^{n}\frac{1}{k^2\binom{2k}{k}}\right]$.

(7) $\sum_{k=0}^{n}\frac{1}{\binom{n}{k}^2}=\frac{3(n+1)^2}{2n+3}\frac{1}{\binom{2n+2}{n+1}}\sum_{k=1}^{n+1}\binom{2k}{k}\frac{1}{k}$.

(8) $\sum_{k=0}^{m-1}(-1)^k\binom{m}{k}\binom{m+n-k-1}{n}=\binom{n-1}{m-1}$.

8.4 三阶组合恒等式

和式中含有三个二项式系数的等式,称之为三阶组合恒等式.

(1) $\sum_{k=0}^{2n}(-1)^k\binom{2n}{k}\binom{2x}{x-n+k}\binom{2z}{z-n+k}$

$$=(-1)^n\frac{(n+x+z)!(2n)!(2x)!(2z)!}{(n+x)!(n+z)!(x+z)!n!x!z!},$$ x,z均为非负整数.

(2) $\sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{x}{k}\binom{x}{n-k}$

$$=\binom{x}{n/2}\binom{-x-1}{n/2}\frac{1+(-1)^n}{2}.$$

(3) $\sum_{k=0}^{n}\binom{x}{k}\binom{y}{n-k}\binom{k}{j}=\binom{x}{j}\binom{y+x-j}{n-j}.$

(4) $\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{\binom{z}{k}}{\binom{y}{k}}=\frac{\binom{y-z}{n}}{\binom{y}{n}}.$

(5) $\sum_{k=0}^{n}\binom{n}{k}\frac{\binom{z}{k}}{\binom{x+k}{k}}=\frac{\binom{x+z+n}{n}}{\binom{x+n}{n}}.$

8.5 广义二项式定理

下列公式称为**广义二项式定理**：

(1) Vandermonde 公式

$$[x+y]_n=\sum_{k=0}^{n}\binom{n}{k}[x]_k[y]_{n-k}.$$

(2) Norlund 公式：

$$[x+y]^n=\sum_{k=0}^{n}\binom{n}{k}[x]^k[y]^{n-k}.$$

其中 $$[x]_k=x(x-1)\cdots(x-k+1),$$

$$[x]^k = x(x+1)\cdots(x+k-1).$$

8.6 多项式系数

定义 8.6.1 设 $n=n_1+n_2+\cdots+n_p$，以下形式的数称为多项式系数(multinomial coefficient).

$$\binom{n}{n_1,n_2,\cdots,n_p}=\frac{n!}{n_1!n_2!\cdots n_p!}.$$

定理 8.6.2 多项式展开定理(multinomial expansion theorem)

$$(x_1+x_2+\cdots+x_p)^n = \sum_{\substack{n_i\geqslant 0(i=1,2,\cdots,p)\\ n_1+n_2+\cdots+n_p=n}} \binom{n}{n_1,n_2,\cdots,n_p} x_1^{n_1}x_2^{n_2}\cdots x_p^{n_p}.$$

性质 8.6.3 多项式系数有以下性质：

(1) 多项式系数的组合意义：n 个不同的物体放入 p 个盒子，使第 i 个盒子有 n_i 个物体，$i=1,2,\cdots,p$，这样的方法数为

$$\binom{n}{n_1,n_2,\cdots,n_p},$$

其中 $n_1+n_2+\cdots+n_p=n$.

(2) 递推公式

$$\binom{n}{n_1,n_2,\cdots,n_p}=\sum_{i=1}^{p}\binom{n-1}{n_1,\cdots,n_i-1,\cdots,n_p}.$$

其中 $n_1+n_2+\cdots+n_p=n$.

(3) 多项式系数与二项式系数的关系

$$\sum_{\binom{s_1+s_2+\cdots+s_k=h}{s_1+2s_2+\cdots+ks_k=m}}\binom{h}{s_1,s_2,\cdots,s_k}=\binom{m-1}{h-1}.$$

8.7 Gauss 二项式系数

定义 8.7.1 设 F_q 为 q 个元素的有限域，$V_n(F_q)$ 为 F_q 上的 n 维线性空间，则 $V_n(F_q)$ 中 k 维子空间的个数记作

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)},$$

$\begin{bmatrix} n \\ k \end{bmatrix}_q$ 称为 **Gauss 系数**(Gauss coefficients).

性质 8.7.2

(1) $\lim\limits_{q\to 1}\begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k}$.

(2) $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$.

(3) $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k\begin{bmatrix} n-1 \\ k \end{bmatrix}_q$.

8.8 排列数

有以下几类排列数：

(1) **全排列**(total permutation)：n 个元素的全排列数为 $n!$

(2) **选排列**(partial permutation)：从 n 个元素中选 r 个元素的排列数记作 P_n^r 或 $P(n,r)$，且 $P_n^r = p(n,r) = [n]_r = n(n-1)\cdots(n-r+1)$.

(3) **圆周排列**(cyclic permutation)：若循环次序相同的排列看作是同一个排列，称为一个圆周排列. 从 n 个元素中选取 r 个元素的圆周排列数为 $\frac{P_n^r}{r}$.

(4) **可重排列**(permutation with repetition)：从 n 个元素中

选 r 个元素的可重排列数为 n^r.

(5) **相遇问题**(含有 $i_k=k$ 的排列数):在 n 级排列中恰有 r 个数满足 $i_k=k$ 的排列数为

$$N(r)=\frac{n!}{r!}\sum_{k=0}^{n-r}(-1)^k\frac{1}{k!}.$$

(6) **更列问题**(不含 $i_k=k$ 的排列数):在 n 级排列中不含 $i_k=k, k=1,2,\cdots,n$ 的排列数为

$$D_n=\sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)!=n!\sum_{k=0}^{n}(-1)^k\frac{1}{k!}.$$

递推公式

$$D_n=(n-1)(D_{n-1}+D_{n-2}),\quad D_1=0,\quad D_2=1.$$

近似式

$$D_n\approx n!/\mathrm{e},\quad \left|D_n-\frac{n!}{\mathrm{e}}\right|<\frac{1}{n-1}.$$

8.9 组合数

有以下两类组合数:

(1) 从 n 个元素中选取 r 个元素的方法数称为**组合数**(combination),记作 $C(n,r)$ 或 C_n^r,且有

$$C(n,r)=\mathrm{C}_n^r=\binom{n}{r}=\frac{[n]_r}{r!}=\frac{n(n-1)\cdots(n-r+1)}{r!}.$$

(2) 从 n 个元素中选 r 个元素的可重组合数(combination with repetition)记作 $F(n,r)$,且有

$$F(n,r)=\frac{[n]^r}{r!}=\binom{n+r-1}{r}.$$

$F(n,r)$ 满足以下递推公式

$$F(n,r)=F(n,r-1)+F(n-1,r),$$
$$F(n,0)=1, F(1,r)=1.$$

8.10 映射数与序列数

关于映射数有以下结果：

(1) **全体映射数**：设 X,Y 是两个有限集合，$|X|=n$，$|Y|=m$，则全体映射 $f:X\to Y$ 的数目为

$$|Y^X|=m^n.$$

(2) **单映射**(injection)的个数为

$$[m]_n=m(m-1)\cdots(m-n+1).$$

(3) **满射**(surjection)的个数为

$$\begin{aligned}S_{n,m}&=m^n-\binom{m}{1}(m-1)^m+\binom{m}{2}(m-2)^n+\cdots\\&\quad+(-1)^{m-1}\binom{m}{m-1}\\&=m!S(n,m),\end{aligned}$$

其中 $S(n,m)$ 为第二类 Stirling 数(参看 8.12 节)。

(4) 实际依赖于所有变量的函数(指满足以下条件的函数)：$\forall i\in\{1,2,\cdots,n\}$，存在 $\alpha,\beta\in X$ 使 $f(t_1,\cdots,t_{i-1},\alpha,t_{i+1},\cdots,t_n)\neq f(t_1,\cdots,t_{i-1},\beta,t_{i+1},\cdots,t_n)$的个数为 $E(n,m,k)=m^{n^k}-\binom{k}{1}m^{n^{k-1}}+\cdots+(-1)^k m$.

(5) 非减映射的个数

设 $Y=\{y_1,y_2,\cdots,y_m\}$ 为一个有序集，$X=\{x_1,x_2,\cdots,x_n\}$ 且 $x_1<x_2<\cdots<x_n$，若映射 $f:X\to Y$ 满足 $f(x_1)\leqslant f(x_2)\leqslant\cdots\leqslant f(x_n)$，则称 f 是一个非减映射. X 到 Y 的非减映射的个数为

$$\frac{[m]^n}{n!}.$$

(6) (a,b)序列数

由 k 个字母 a 和 m 个字母 b 组成的满足以下性质的序列：对

任意的 $i(1\leqslant i\leqslant m+k)$，在序列的前 i 项中字母 a 的个数不少于字母 b 的个数，所有具有此性质的序列数为 $\frac{k-m+1}{k+1}\binom{m+k}{m}$.

8.11 第一类 Stirling 数

定义 8.11.1 设

$$[x]_n=\sum_{k=0}^{n}s(n,k)x^k,$$

其中系数 $s(n,k)$ 称为**第一类 Stirling 数**. 它的表达式为

$$s(n,k)=(-1)^k\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n-1}i_1i_2\cdots i_k.$$

数表见表 8.1.

表 8.1 第一类 Stirling 数 $s(n,k)$

$s(n,k)$ n \ k	0	1	2	3	4	5	6	7
1	0	1	0					
2	0	−1	1	0				
3	0	2	−3	1	0			
4	0	−6	11	−6	1	0		
5	0	24	−50	35	−10	1	0	
6	0	−120	274	−225	85	−15	1	0

递推公式 8.11.2

$$s(n+1,k)=s(n,k-1)-ns(n,k)$$

$$s(n,0)=0,\ s(n,n)=1,\ s(n,k)=0(\text{当 } n<k \text{ 时}).$$

第一类 Stirling 数的组合意义：在对称群 S_n 中恰含有 k 个轮

换的置换的个数等于$|s(n,k)|$. 且有

$$[x]^n = \sum_{k=0}^{n} |s(n,k)| x^k$$

定义 8.11.3 设 $\alpha=(a_0,a_1,a_2,\cdots)$是一个无限实数序列,引入记号

$$[x \mid \alpha]_n = (x-a_0)(x-a_1)\cdots(x-a_{n-1}), [x \mid \alpha]_0 = 1.$$

则展式

$$[x \mid \alpha]_n = \sum_{k=0}^{n} s_\alpha(n,k) x^k$$

中系数 $s_\alpha(n,k)$称为**推广的第一类 Stirling 数.**

8.12 第二类 Stirling 数

定义 8.12.1 设

$$t^n = \sum_{k=0}^{n} S(n,k)[t]_k,$$

则系数 $S(n,k)$就称为**第二类 Stirling 数**. 它的表达式为

$$S(n,m) = \frac{1}{m!}\sum_{k=0}^{m-1}(-1)^k\binom{m}{k}(m-k)^n.$$

数表见表 8.2.

递推公式 8.12.2

(1) $S(n+1,k) = S(n,k-1) + kS(n,k)$,

$$S(n,1) = S(n,n) = 1.$$

(2) $S(n+1,m) = \sum_{k=m-1}^{n}\binom{n}{k}S(k,m-1)$,

$$S(n,1) = 1.$$

第二类 Stirling 数的组合意义:

(1) n 元集合划分为 k 类的划分数恰为 $S(n,k)$.

(2) n 元集合 X 到 m 元集合 Y 的满射个数为 $m!S(n,m)$.

表 8.2　第二类 Stirlng 数 $S(n,k)$

$S(n,k)$ \ k / n	0	1	2	3	4	5	6	7	8	9	10
1	1										
2	1	1									
3	1	3	1								
4	1	7	6	1							
5	1	15	25	10	1						
6	1	31	90	65	15	1					
7	1	63	301	350	140	21	1				
8	1	127	966	1701	1050	266	28	1			
9	1	255	3025	7770	6951	2646	462	36	1		
10	1	511	9330	34105	42525	2282	5880	750	45	1	

定义 8.12.3　函数

$$\frac{1}{k!}(e^t-1)^k=\sum_{n=k}^{\infty}\frac{S(n,k)}{n!}t^n,$$

称为第二类 Stirling 数的生成函数.

公式 8.12.4

关于第二类 Stirling 数有以下等式:

(1) $S(n,2)=2^{n-1}-1$.

(2) $S(n,n-1)=\binom{n}{2}$.

(3) $S(n,n-2)=\binom{n}{3}+3\binom{n}{4}$.

(4) $S(n,n-3)=\binom{n}{4}+10\binom{n}{5}+15\binom{n}{6}$.

(5) $1-S(n,2)+2!\,S(n,3)-3!\,S(n,4)+\cdots$

$$+(-1)^{n-1}(n-1)!=0.$$

定义 8.12.5

由定义 8.11.3 中的记号$[x|\alpha]_n$，设

$$x^n \equiv \sum_{k=0}^{n} S_\alpha(n,k)[x\mid\alpha]_n,$$

其中系数 $S_\alpha(n,k)$称为**第二类推广的 Stirling 数**.

定义 8.12.6 设

$$\frac{t^k}{(1-a_0t)(1-a_1t)\cdots(1-a_kt)}=\sum_{n=k}^{\infty}S_\alpha(n,k)t^n.$$

则称它为**第二类推广的 Stirling 数的生成函数**.

8.13 Bell 数

定义 8.13.1 n 元集合的所有划分数称为 **Bell 数**，记作 B_n，即它有以下的表达式：

$$B_n=\sum_{k=1}^{n}S(n,k),$$

$$B_{n+1}=\frac{1}{\mathrm{e}}\left(1^n+\frac{2^n}{1!}+\frac{3^n}{2!}+\cdots\right).$$

公式 8.13.2 Bell 数满足以下的递推公式：

$$B_{n+1}=\sum_{k=0}^{n}\binom{n}{k}B_k,\quad B_0=1.$$

定义 8.13.3 函数

$$\mathrm{e}^{\mathrm{e}^t-1}=\sum_{n=0}^{\infty}\frac{B_n}{n!}t^n,$$

称为 **Bell 数的生成函数**.

Bell 数的数表如表 8.3.

表 8.3 Bell 数 B_n

n	0	1	2	3	4	5	6	7	8	9	10
B_n	1	1	2	5	15	52	203	877	4140	21147	115975

8.14 Fibonacci 数

定义 8.14.1 集合$[1,n]=\{1,2,\cdots,n\}$的不包含相邻整数的子集的个数,包括空集,总数记作 F_{n+1},称为 **Fibonacci 数**.

F_n 可表为

$$F_n=\sum_{k=0}^{\lfloor \frac{n}{2}\rfloor}\binom{n-k}{k}.$$

它满足以下递推公式

$$F_{n+1}=F_n+F_{n-1},\quad F_0=F_1=1.$$

F_n 还可表示为以下形式

$$F_n=\frac{\alpha^{n+1}-\beta^{n+1}}{\sqrt{5}}=\|\alpha^{n+1}/\sqrt{5}\|,$$

其中 $\alpha=\frac{1+\sqrt{5}}{2}$,$\beta=\frac{1-\sqrt{5}}{2}$,$\|x\|$ 表示与 $x\left(x\neq m+\frac{1}{2},m\in\mathbf{Z}\right)$最接近的整数. Fibonacci 数表见表 8.4.

定义 8.14.2 设

$$\rho=\lim_{n\to\infty}\frac{F_n}{F_{n+1}}=\frac{1}{\alpha}=-\beta=\frac{\sqrt{5}-1}{2}=0.61803\cdots$$

称 ρ 为**黄金分割数或黄金率**(golden section number).

公式 8.14.3 关于 Fibonacci 数有以下恒等式:

(1) $F_n^2=F_{n-1}\cdot F_{n+1}+(-1)^n,\quad n\geqslant 2.$

(2) $F_{m+n}^2-F_{m-n}^2=F_{2m}F_{2n}.$

(3) $\sum_{i=0}^{n} F_i = F_{n+2} - 1.$

(4) $\sum_{i=0}^{2n} F_i = F_{2n+1}.$

(5) $\sum_{i=0}^{n} F_i^2 = F_n F_{n+1}.$

定义 8.14.4 函数

$$\frac{1}{1-x-x^2} = \sum_{k=0}^{\infty} F_k x^k,$$

称为 **Fibonacci 数的生成函数.**

例 8.14.5 Fibonacci 数的生物繁殖模型 设一对雌雄兔子出生两个月后开始每月生下一对雌雄幼兔. 如果开始时有一对刚出生的幼兔,问第 n 个月时有多少对兔子?

该问题可分析如下:设第 n 个月时有兔子 F_n 对,它们由两部分组成:一部分为第 $n-1$ 个月时已经存在的兔子,为 F_{n-1} 对;另一部分为新出生的兔子,它们是由第 $n-2$ 个月时已经存在的兔子生下的,为 F_{n-2} 对. 故有

$$F_n = F_{n-1} + F_{n-2}, \quad F_0 = F_1 = 1.$$

定义 8.14.6 设 Y 是$[1,n]$的有以下性质的子集: $\forall i,j \in Y$ 有 $|i-j| \geq l+1$,其中 l 为非负整数. $[1,n]$中所有这样的子集的个数 $F_{n,l}$ 称为**广义 Fibonacci 数**(extended Fibonacci number). 且有

$$F_{n+1,l} = \sum_{k\geq 0} \binom{n-lk+l}{k}.$$

定义 8.14.7 函数

$$\frac{1}{1-t-t^{l+1}} = \sum_{n=0}^{\infty} F_{n,l}\, t^n,$$

称为广义 Fibonacci 数的生成函数.

8.15 Lucas 数

定义 8.15.1 集合[1,n]的不相邻圆周子集(即不包含相邻整数,也不同时包含 1 和 n 的子集),包括空集,其总数称为 **Lucas 数**,记作 F_n^*,且

$$F_n^* = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-k}\binom{n-k}{k}.$$

它满足以下递推公式

$$F_{n+1}^* = F_n^* + F_{n-1}^*,\ F_1^* = 1,\ F_2^* = 3.$$

因此,Lucas 数与 Fibonacci 数有相同的递推公式,只是初值不同.

定义 8.15.2 函数

$$\frac{t+2t^2}{1-t-t^2} = \sum_{n\geqslant 1} F_n^* t^n,$$

称为**广义 Lucas 数的生成函数**.

它有以下表达式

$$F_n^* = \alpha^n + \beta^n,$$

其中 $\alpha=(1+\sqrt{5})/2$, $\beta=(1-\sqrt{5})/2$.

定义 8.15.3 设[1,n]中具有以下性质的子集 Y: $\forall\, i,j\in Y$ 有 $\min(|i-j|, n-|i-j|)>l+1$,l 为非负整数,所有这样的子集,包括空集,总数记作 $F_{n,l}^*$,称为**广义 Lucas 数**(extended Lucas number). 且有

$$F_{n,l}^* = \sum_{k\geqslant 0} \frac{n}{n-kl}\binom{n-kl}{k}.$$

定义 8.15.4 函数

$$\frac{1+(l+1)t^{l+1}}{1-t-t^{l+1}} = \sum_{n\geqslant 1} F_{n,l}^* t^n.$$

称为广义 Lucas 数的生成函数.

Lucas 数表见表 8.4.

表 8.4 Fibonacci 数 F_n 与 Lucas 数 F_n^*

n	0	1	2	3	4	5	6	7	8	9	10
F_n	1	1	2	3	5	8	13	21	34	55	89
F_n^*		1	3	4	7	11	18	29	47	76	123

8.16 Catalan 数

定义 8.16.1 设 C_n 为 Catalan 数,它有以下三种互相等价的定义:

(1) 将正 n 边形 $A_1A_2\cdots A_n$ 用对角线剖分为三角形的方法数为 C_n.

(2) n 个数的乘积:$a_1a_2\cdots a_n$ 的不同结合方法数为 C_{n+1}.

(3) 在整数坐标平面的格子上,从点$(0,0)$到点(n,n)由垂直线段和水平线段组成的路径,且要求中间点(a,b)满足 $a\leqslant b$,所有这样的路径数为 C_{n+2}.

它有以下表达式

$$C_n=\frac{1}{n-1}\binom{2n-4}{n-2},\quad n\geqslant 2.$$

公式 8.16.2 递推公式

(1) $C_{n+1}=C_2C_n+C_3C_{n-1}+\cdots+C_nC_2\,(n\geqslant 2)$, $C_2=1$.

(2) $(n-3)C_n=\dfrac{n}{2}\sum\limits_{k=3}^{n-1}C_kC_{n-k+2}\quad(n\geqslant 4)$, $C_2=1$, $C_3=1$.

定义 8.16.3 函数

$$\frac{1-\sqrt{1-4x}}{2x}=\sum_{k=0}^{\infty}C_{k+2}x^{k},$$

称为 **Catalan 数的生成函数**.

表 8.5 为 Catalan 数表.

表 8.5 Catalan 数 C_n

n	2	3	4	5	6	7	8	9	10
C_n	1	1	2	5	14	42	132	429	1430

8.17 Ramsey 数

定理(定义)8.17.1 设 $q_1,q_2,\cdots,q_n,t$ 为满足 $q_i\geqslant t(i=1,2,\cdots,n)$ 的正整数,则存在仅依赖于 $q_1,q_2,\cdots,q_n,t$ 的最小正整数 $\gamma=\gamma(q_1,q_2,\cdots,q_n,t)$:对于任何 $|X|\geqslant\gamma$ 的集合 X,当把 X 的所有 t 元子集放入 n 个有序的盒子里时,必有某个 $i(1\leqslant i\leqslant n)$,使第 i 个盒子里包含某 q_i 个元素的全部 t 元子集. 数 $\gamma(q_1,q_2,\cdots,q_n,t)$ 称为 Ramsey 数.

当 $n=2$ 时记作 $\gamma(k,l)$. 与 Ramsey 图相对应,详见定义 10.10.4.

性质 8.17.2 Ramsey 数的性质

(1) $\gamma(k,l)=\gamma(l,k)$.

(2) $\gamma(k,l)\leqslant\gamma(k,l-1)+\gamma(k-1,l)$.

(3) 若 $\gamma(k,l-1)$,$\gamma(k-1,l)$ 均为偶数,则 $\gamma(k,l)\leqslant\gamma(k,l-1)+\gamma(k-1,l)-1$.

(4) $2^{k/2}\leqslant\gamma(k,l)\leqslant\binom{k+l-2}{k-1}$.

(5) $\gamma(q_1,q_2,\cdots,q_n)\leqslant\gamma(q_1-1,q_2,\cdots,q_n)+\gamma(q_1,q_2-1,\cdots,$

$q_n)+\cdots+\gamma(q_1,\cdots,q_{n-1},q_n-1)-n+2$.

(6) $\gamma(q_1+1,\cdots,q_n+1)\leqslant\dfrac{(q_1+q_2+\cdots+q_n)!}{q_1!\ q_2!\ \cdots q_n!}$.

表 8.6 为已知的 $\gamma(k,l)$ 或其上下界.

表 8.6 已知的 $\gamma(k,l)$ 或其上下界

$\gamma(k,l)$ k \ l	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2		2	3	4	5	6	7	8	9	10	11	12	13	14	15
3			6	9	14	18	23	28	36	40 43	46 51	51 60	59 69	66 78	73 89
4				18	25	35 41	49 61	53 84	69 115	80 149	96 191	106 238	118 291	129 349	134 417
5					43 49	58 87	80 143	95 216	114 317	442					
6						102 165	298	495	780	1171					
7							205 540	1031	1713	2826					
8								1870	282 3583	6090					
9									6625	565 12715					
10										798 23854					

（摘自 Bollobás 的新著 MODERN GRAPH THEORY(1998)）

8.18 Lah 数

定义 8.18.1 设

$$[-x]_n = \sum_{k\geqslant 0} L_{n,k}[x]_k,$$

则系数 $L_{n,k}$ 称为 Lah 数. 它与 Stirling 数有密切的关系.

它有以下表达式

$$L_{n,k} = (-1)^n \frac{n!}{k!}\binom{n-1}{k-1}, \quad n,k \geqslant 0.$$

性质 8.18.2

(1) $[x]_n = \sum_{k\geqslant 0} L_{n,k}[-x]_k$.

(2) $\sum_{k\geqslant 0} L_{n,k}L_{k,m} = \delta_{n,m}$.

(3) $L_{n,k} = \sum_{j\geqslant 0}(-1)^j s(n,j)S(j,k)$.

其中 $s(n,j)$ 为第一类 Stirling 数, $S(j,k)$ 为第二类 Stirling 数.

公式 8.18.3 递推公式

$$L_{n+1,k} = -(n+k)L_{n,k} - L_{n,k-1}.$$

$$L_{0,0} = 1, L_{n,k} = 0 (\text{当 } n < k).$$

由此可得 $L_{n,0}=0(n>0)$, $L_{n,n}=(-1)^n$.

定义 8.18.4 函数

$$\frac{1}{k!}\left(\frac{-x}{1+x}\right)^k = \sum_{n\geqslant 0} L_{n,k}\frac{x^n}{n!},$$

称为 Lah 数的生成函数.

表 8.7 为 Lah 数表.

表 8.7 Lah 数 $L_{n,k}$

$L_{(n,k)}$ n \ k	0	1	2	3	4	5	6
0	1						
1	0	−1					
2	0	2	1				
3	0	−6	−6	−1			
4	0	24	36	12	1		
5	0	−120	−240	−120	−20	−1	
6	0	720	1800	1200	300	30	1

8.19 Bernoulli 数和 Euler 数

定义 8.19.1 设

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n^*}{n!} x^n,$$

则系数 B_n^* 称为 Bernoulli 数.

它满足以下递推公式

$$B_{n-1}^* = -\frac{1}{n} \sum_{k=0}^{n-2} \binom{n}{k} B_k^*, \quad B_{2n+1}^* = 0 (n \geqslant 1).$$

定义 8.19.2 设

$$x^n = \sum_{k=0}^{n} \binom{x+k-1}{n} A_{n,k},$$

则称 $A_{n,k}$ 为 Euler 数,且有

$$A_{n,k} = \sum_{j=1}^{k} (-1)^j \binom{n+1}{j} (k-j)^n.$$

9 组合计数方法与问题

9.1 初等计数原理

定理 9.1.1 加法原理(addition principle) 设 A,B 是某集合的两个有限子集,且 $A\cap B=\varnothing$,则

$$|A\cup B|=|A|+|B|.$$

定理 9.1.2 乘法原理(multiplication principle) 设 A,B 是两个有限集合,$A\times B=\{(a,b)\mid a\in A,b\in B\}$,则

$$|A\times B|=|A|\cdot|B|.$$

定理 9.1.3 鸽子笼原理(pigeon hole principle) 把 $n+1$ 件东西放入 n 个盒子,则至少有一个盒子含有两件或更多的东西.

定理 9.1.4 加强的鸽子笼原理(augmenting pigeon hole principle) 设 $q_1,q_2,\cdots,q_n$ 都是正整数,如果把 $q_1+q_2+\cdots+q_n-n+1$ 件东西放入 n 个盒子,则必有某一个 $i(1\leqslant i\leqslant n)$ 使第 i 个盒子至少包含 q_i 件东西.

9.2 包含与排斥原理

包含与排斥原理又称容斥原理,它给出一些有限子集的并集与交集之间的关系. 如果在某些问题里,子集的交集的元素个数容易求得,则可通过包含与排斥原理求出子集的并集的元素的个数. 反之亦然.

原理 9.2.1 包含与排斥原理(简单形式)(inclusion and exclusion principle) 设 S 是一个集合,$A_1,A_2,\cdots,A_q$ 是 S 的一

些有限子集，则有

$$|\bigcup_{i=1}^{q} A_i| = \sum_{i=1}^{q} |A_i| - \sum_{1\leqslant i<j\leqslant q} |A_i \cap A_j| + \cdots + (-1)^{q+1} |\bigcap_{i=1}^{q} A_i|,$$

$$|\bigcap_{i=1}^{q} A_i| = \sum_{i=1}^{q} |A_i| - \sum_{1\leqslant i<j\leqslant q} |A_i \cup A_j| + \cdots + (-1)^{q+1} |\bigcup_{i=1}^{q} A_i|.$$

原理 9.2.2　包含与排斥原理(带权形式)　设 S 是一个集合，$\forall x \in S$ 定义权函数(取正值的函数)$m(x)$，$A_1, A_2, \cdots, A_q$ 为 S 的有限子集，子集 A 的权定义为 $m(A) \triangleq \sum_{x\in A} m(x)$，令 $Q = \{1, 2, \cdots, q\}$，则有

$$m(\bigcup_{i\in Q} A_i) = \sum_{k=1}^{q} (-1)^{k+1} \sum_{\substack{K\subseteq Q\\ |K|=k}} m(\bigcap_{i\in K} A_i).$$

$$m(\bigcap_{i\in Q} A_i) = \sum_{k=1}^{q} (-1)^{k+1} \sum_{\substack{k\subseteq Q\\ |K|=k}} m(\bigcup_{i=K} A_i)$$

定理 9.2.3　Sylvester 公式(Sylvester formula)　设 $A_1, A_2, \cdots, A_q$ 为有限集合 X 的子集，则 X 中所有不属于任何一个 A_i 的元素的集合的权等于

$$M_q^0 = m(X) + \sum_{K\subseteq Q} (-1)^{|K|} m(\bigcap_{i\in K} A_i).$$

定理 9.2.4　Jordan 筛法公式(Jordan sieve formula)　设 $A_1, A_2, \cdots, A_q$ 为有限集合 X 的子集，则 X 中所有属于 p 个集合 A_i 的元素的集合的权为

$$M_q^p = \sum_{k=p}^{q} (-1)^{k-p} \binom{k}{p} \sum_{\substack{K\subset Q\\ |K|=k}} m(\bigcap_{i\in K} A_i).$$

当 $p=0$ 时即为定理 9.2.3，这时在公式中取

$$m(\bigcap_{i\in\varnothing} A_i) = m(X).$$

例 9.2.5　确定欧拉 φ-函数 $\varphi(n)$(Euler φ-function)　小于 n 且与 n 互素的正整数的个数.

解 设 n 的素因子标准分解式为

$$n = p_1^{t_1} p_2^{t_2} \cdots p_q^{t_q},$$

令 A_i 为不大于 n 且是 p_i 的倍数的正整数的集合，则

$$|A_i| = \frac{n}{p_i}, \ |A_i \cap A_j| = \frac{n}{p_i p_j}, \cdots$$

由 Sylvester 公式(定理 9.2.3)可得

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_q}\right).$$

例 9.2.6 求不大于某个给定的正整数 n，而可被某些正整数 $n_1, n_2, \cdots, n_q$ 中任一个整除的正整数的个数.

方法类似于例 9.2.5.

应用包含与排斥原理可证明以下结果：

例 9.2.7 求不含不动点的 n 次置换的个数，见问题 9.4.2.

例 9.2.8 求实际依赖于所有变量的函数的个数，见 8.10 节之(4).

例 9.2.9 确定图中不含 k 团时最大边数的界. 见(定理 10.3.7).

例 9.2.10 确定满射个数(见 8.10 节之(3))

例 9.2.11 **夫妇入座问题** 设 n 个丈夫(用 $1,2,\cdots,n$ 表示)和他们的妻子(用 $\bar{1},\bar{2},\cdots,\bar{n}$ 表示)，要求他们男女交替围坐在一张圆桌旁，且没有一个妻子坐在她的丈夫旁，求当丈夫坐完后，妻子的坐法数.

解 设 $X=\{1,2,\cdots,n\}$，$Y=\{\bar{1},\bar{2},\cdots,\bar{n}\}$，$S$ 为全体 X 到 Y 的双射的集合. 令

$$A_{2i-1} = \{f \in S \mid f(i) = \bar{i}\},$$

$$A_{2i} = \{f \in S \mid f(i) = \overline{i+1}\},$$

$$A_{2n} = \{f \in S \mid f(n) = \bar{1}\},$$

则符合要求的入座法数目为

$$T(n)=|S|-|\bigcup_{i=1}^{2n}A_i|$$

$$=n!-\sum_{k\subseteq\{1,2,\cdots,2n\}}(-1)^{|K|-1}|\bigcap_{i\in K}A_i|.$$

又如果 $K\subseteq\{1,2,\cdots,2n\}$ 中包含相邻圆周整数，则 $|\bigcap_{i\in K}A_i|=0$；反之，由不相邻圆周 k 子集的数目(看例 9.3.3)，得

$$\sum_{k\subseteq\{1,2,\cdots,2n\}}(-1)^{|K|-1}|\bigcap_{i\in K}A_i|=(-1)^{|K|}\frac{2n}{2n-k}\binom{2n-k}{k}(n-k)!$$

综上，得

$$T(n)=n!-\frac{2n}{2n-1}\binom{2n-1}{1}(n-1)!$$

$$+\frac{2n}{2n-2}\binom{2n-2}{2}(n-2)!+\cdots+(-1)^n\cdot 2.$$

$T(2)=0, T(3)=1, T(4)=2, T(5)=13.$

9.3 有限集的子集的计数问题

例 9.3.1 $[1,n]$中不包含相邻整数的 k 子集的个数为

$$f(n,k)=\binom{n-k+1}{k}.$$

例 9.3.2 $[1,n]$中所有不包含相邻整数的子集，包括空集，总数为 Fibonacci 数 F_n(见定义 8.14.1)，即

$$F_n=\sum_{k\geqslant 0}\binom{n-k+1}{k}.$$

例 9.3.3 $[1,n]$中不包含相邻整数，也不同时包含 n 和 1 的 k 子集称为不相邻圆周 k 子集，其个数为

$$f^*(n,k)=\frac{n}{n-k}\binom{n-k}{k}.$$

例 9.3.4 $[1,n]$中所有不相邻圆周子集，包括空集，总数为 Lucas 数(见定义 8.15.1)即

$$F_n^* = \sum_{k\geq 0} \frac{n}{n-k}\binom{n-k}{k}.$$

例 9.3.5 设 S 是 n 元集，S 中关于子集的包含关系两两不可比较的子集的最大个数为

$$\binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

9.4 置换的计数问题

问题 9.4.1 设 S_n 是 n 次对称群，置换 $\sigma \in S_n$ 的标准轮换分解式中含有长度为 k 的轮换有 λ_k 个($k=1,2,\cdots,n$)且 $1\cdot\lambda_1+2\cdot\lambda_2+\cdots+n\cdot\lambda_n=n$，则称 σ 是一个 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$-型置换. S_n 中 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$-型置换的个数为

$$\frac{n!}{1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\cdot\lambda_1!\lambda_2!\cdots\lambda_n!}.$$

问题 9.4.2 设 $\sigma \in S_n$，若有 $i \in \{1,2,\cdots,n\}$ 使 $\sigma(i)=i$，则称 i 是 σ 的一个不动点. S_n 中没有不动点的置换个数为

$$D(n) = (n)!\left(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^n\frac{1}{n!}\right).$$

且有递推式

$$D(n) = nD(n-1)+(-1)^n, D(1)=0.$$

问题 9.4.3 S_n 中恰有 p 个不动点的置换个数为

$$\binom{n}{p}D(n-p).$$

问题 9.4.4 S_n 中恰含有 k 个轮换的置换个数为

$$c(n,k) = |s(n,k)| = (-1)^{n+k}s(n,k).$$

其中 $s(n,k)$ 为第一类 Stirling 数(见 8.11 节)．且有递推式

$$c(n,k)=c(n-1,k-1)+(n-1)c(n-1,k),$$
$$c(n,0)=0,c(n,n)=1.$$

9.5 集合的划分数

定义 9.5.1 设 X 是一个集合，$A_1,A_2,\cdots,A_q$ 是 X 的非空子集，并满足

(1) $A_i\cap A_j=\varnothing$，对任何 $i\neq j$；

(2) $\bigcup_{i=1}^{q}A_i=X$，

则称 $A_1,A_2,\cdots,A_q$ 是 X 的一个**划分**(partition)，每一个子集 A_i 称为这个划分的一个**类**(class)．

定义 9.5.2 集合$[1,n]$划分为 m 类的方法数，称为**划分数**，等于第二类 Stirling 数(见 8.12 节)：

$$S(n,m)=\frac{1}{m!}S_{n,m}=\frac{1}{m!}\sum_{k=0}^{m-1}(-1)^k\binom{m}{k}(m-k)^n.$$

定理 9.5.3 集合$[1,n]$的所有划分数等于 Bell 数(见 8.13 节)：

$$B_n=S(n,1)+S(n,2)+\cdots+S(n,n).$$

定理 9.5.4 把$[1,n]$划分为 $k+r$ 类，使 $1,2,\cdots,k$ 分别属于不同的类，这样的划分数称为**指定 k 元划分数**，总数为 $\sum_{p=r}^{n-k}\binom{n-k}{p}S(p,r)k^{n-k-p}$.

定理 9.5.5 把$[1,n]$划分为含有 1 个元素的 λ_1 类，含有 2 个元素的 λ_2 类，…，含有 n 个元素的 λ_n 类，且 $1\cdot\lambda_1+2\cdot\lambda_2+\cdots+n\cdot\lambda_n=n$，这样的划分数称为 **$1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 型划分**，总数为

$$N(1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n})=\frac{n!}{\lambda_1!\lambda_2!\cdots\lambda n!(1!)^{\lambda_1}(2!)^{\lambda_2}\cdots(n!)^{\lambda_n}}.$$

9.6 整数的分拆数

定义 9.6.1 设 n 为正整数，有正整数 $n_1, n_2, \cdots, n_m$ 满足

(1) $n = n_1 + n_2 + \cdots + n_m$;

(2) $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_m \geqslant 1$.

则称 $n_1, n_2, \cdots, n_m$ 为 n 的一个**分拆**(partition).

定理 9.6.2 $P(n,m)$为整数 n 分拆为 m 部分的分拆数，目前尚无简单的直接表达式. 仅有以下结果：

(1) 递推式

$$P(n+k,k) = P(n,1) + P(n,2) + \cdots + P(n,k),$$

$$P(n,1) = P(n,n) = 1, P(n,k) = 0 \quad (当\ n < k).$$

(2) 生成函数

$$F_2(x) = x^m(1-x)^{-1}(1-x^2)^{-1}\cdots(1-x^m)^{-1} = \sum_{n=m}^{\infty} P(n,m)x^n.$$

$$Z\left(S_m; \frac{xy^2}{1-xy}\right) = \sum_{n=m}^{\infty} P(n,m)x^n y^{n+m},$$

其中 $Z(S_m;t)$为对称群 S_m 的循环指标(见 9.8 节).

定理 9.6.3 设 $P(n)$为 n 的全部分拆数，则

$$P(n) = P(n,1) + P(n,2) + \cdots + P(n,n).$$

并有以下性质：

(1) 渐近式

$$P(n) < e^{\sqrt{\frac{20}{3}n}}.$$

(2) 生成函数

$$F_1(x) = \prod_{i=1}^{\infty}(1-x^i)^{-1} = \sum_{n=0}^{\infty} P(n)x^n.$$

其中规定 $P(0)=1$.

表 9.1 为整数 n 分拆为 k 部分的分拆数 $P(n,k)$ 及分拆总数 $P(n)$.

表 9.1　分拆数 $P(n,k)$ 及分拆总数 $P(n)$

$P(n,k)$ \ k / n	1	2	3	4	5	6	7	8	9	10	$P(n)$
1	1										1
2	1	1									2
3	1	1	1								3
4	1	2	1	1							5
5	1	2	2	1	1						7
6	1	3	3	2	1	1					11
7	1	3	4	3	2	1	1				15
8	1	4	5	5	3	2	1	1			22
9	1	4	7	6	5	3	2	1	1		30
10	1	5	8	9	7	5	3	2	1	1	42

性质 9.6.4　分拆的性质：

(1) 分拆的共轭性与 Ferrers 图　将 $n=7$ 的一个分拆 $7=3+2+1+1$ 画成图 9.1 所示的方格图：

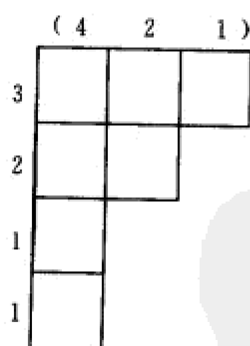


图　9.1

图 9.1 称为分拆 $7=3+2+1+1$ 的 Ferrers 图(Ferrers graphic). 从图上可见,每一列的方格数对应着 7 的另一个分拆：$7=4+2+1$. 这两个分拆称为**互相共轭的**. 若一个分拆与它的共轭分拆相等,就称为它是**自共轭分拆**. 例如 $6=3+2+1$ 就是一个自共轭分拆. 自共轭分拆的 Ferres 图是关于对角线对称的.

(2) n 的最大部分为 k 的分拆数等于 n 分为 k 部分的分拆数(由 Ferrers 图易见).

(3) n 分为两两不同的奇数的分拆数等于 n 的自共轭分拆数.

利用 Ferrers 图可建立互相共轭的两类分拆集合之间的一一对应关系：设 $n=(2k_1+1)+(2k_2+1)+\cdots,k_1>k_2>\cdots$ 为第一类的一个分拆，做以下的一个对称 Ferrers 图：

第 1 行与第 1 列：k_1+1 个方格；

第 2 行与第 2 列：k_2+1 个方格；

……

由此得到一个 n 的自共轭分拆. 反之，由任一个自共轭分拆可对应一个第一类分拆.

(4) n 划分为两两不同的划分数等于 n 分拆为各部分都是奇数的分拆数.

利用 Ferrers 图可以建立这两类分拆的一一对应关系：设 n 的一个各部分均为奇数的分拆：$n=\underbrace{(2k_1+1)+\cdots+(2k_1+1)}_{p个}+\cdots$

将每一个奇数(例如 $2k_1+1$ 的个数)p 表为：

$$P=2^{i_1}+2^{i_2}+\cdots,\quad i_1>i_2>\cdots\geqslant 0.$$

做 n 的 Ferrers 图如下：

第 1 行为$(2k_1+1)2^{i_1}$个方格；

第 2 行为$(2k_1+1)2^{i_2}$个方格；

……

则可得到 n 的一个各部分不相同的分拆. 反之亦然.

(5) $Q_1(n)$与 $Q_2(n)$的关系　设 $Q_1(n)$为 n 分拆为奇数个互不相同部分的分拆数，$Q_2(n)$为 n 分拆为偶数个互不相同部分的分拆数，则

$$Q_2(n)=\begin{cases}Q_1(n)+(-1)^k, n=\dfrac{3k^2\pm k}{2},\\ Q_1(n), \qquad n\neq\dfrac{3k^2\pm k}{2}.\end{cases}$$

利用 Ferrers 图可以对这两类分拆进行变换.

(6) n 分拆为两两不同的部分的分拆数　设 $Q(n)$ 为 n 分拆成两两不同的部分的分拆数,则

$$Q(n)=\sum_{k\geqslant 0}(-1)^{\binom{k+1}{2}}P\left(2n-\binom{k+1}{2}\right),$$

且有生成函数

$$F_3(x)=\prod_{k=1}^{\infty}(1+x^k)=\prod_{k=1}^{\infty}(1-x^{2k-1})^{-1}=\sum_{n=0}^{\infty}Q(n)x^n,$$

其中规定 $Q(0)=1$.

(7) n 分拆为各部分都是偶数的分拆数　设 $n=2k$ 为偶数,它分拆为各部分都是偶数的分拆数等于 $P(k)$($P(k)$ 为 k 的全部分拆数).

(8) n 分拆为两两不同的奇数的分拆数 $Q_3(n)$,它的生成函数为

$$\prod_{k=0}^{\infty}(1+x^{2k+1})=\sum_{n=0}^{\infty}Q_3(n)x^n,$$

其中规定 $Q_3(0)=1$.

(9) n,m,h 分拆　把 n 分为 m 部分,其最小部分为 h 的分拆数,记作 $P(n,m|h)$,则有递推公式:

$$P(n,m\mid 1)=P(n-1,m-1)-1;$$

$$P(n,m\mid h)=P(n-m,m\mid h-1), h>1.$$

(10) n,h 分拆　在 n 的所有分拆中最小部分为 h 的分拆数记作 $P(n|h)$. 有以下递推公式:

$$P(n\mid 1)=P(n-1);$$

$$P(n\mid h)=P(n-1\mid h-1)-P(n-h\mid h-1),$$

其中 $h>1$.

9.7 Burnside 引理

用群的方法解决某些计数问题可以得到很好的结果，特别是计算某些组合结构的等价类，这些等价类正好可用群对集合的作用的轨道来表示，因而可把问题转换为计算轨道数的问题.

定义 9.7.1 设 G 是一个群，X 是一个集合，若对任一个 $g\in G$ 都对应于 X 上的一个函数 $g(x)$，满足

(1) $e(x)=x, \forall x\in X$;

(2) $(g_1g_2)(x)=g_1(g_2(x)), \forall x\in X$.

则称 $g(x)$ 是 G 对 X 的**作用**(action). 称 G **作用于** X.

定义 9.7.2 设群 G 作用于集合 X 上，$a\in X$，令

$$\Omega_a = \{g(a) \mid g \in G\},$$

称 Ω_a 为 a 所在的 G **轨道**(Orbit).

定义 9.7.3 设群 G 作用于集合 X 上，若 $a\in X, g\in G$，满足

$$g(a) = a,$$

则称 a 是 g 的一个**不动点**(fixed point).

定理 9.7.4 Burnside 引理(Burnside lemma) 设有限群 G 作用于有限集合 X 上，则 X 在 G 作用下的轨道数目为

$$N = \frac{1}{|G|}\sum_{g\in G}\chi(g),$$

其中 $\chi(g)$ 为 g 在 X 上的不动点的个数，即

$$x(g) = |\{a \in X \mid g(a) = a\}|.$$

定理 9.7.5 Burnside 引理的带权形式(weighted form of Burnside lemma) 设有限群 G 作用于有限集合 X 上，$\forall x\in X$，定义权函数 $w(x)$ 满足 $w(g(x))=w(x), g\in G$. 轨道的权定义为 $w(\Omega_a)=w(a)$. 若 X 在 G 作用下的全部轨道为 $\Omega_1, \Omega_2, \cdots, \Omega_N$，

则有

$$\sum_{i=1}^{N} w(\Omega_i) = \frac{1}{|G|}\sum_{g\in G}\sum_{\substack{x\in X\\ g(x)=x}} w(x),$$

其中和式 $\sum_{\substack{x\in X\\ g(x)=x}} w(x)$ 表示求 g 的所有不动点的权之和.

9.8 置换群的轮换指标

定义 9.8.1 设 G 是一个 n 次置换群,多项式

$$Z(G;t_1,t_2,\cdots,t_n) = \frac{1}{|G|}\sum_{\substack{g\in G\\ g\text{是}1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\text{型}}} t_1^{\lambda_1(g)} t_2^{\lambda_2(g)}\cdots t_n^{\lambda_n(g)},$$

称为 G 的**轮换指标或循环指标**(cyclic index). 其中和式是对每个 G 中的元素求和. 记号 $Z(G;t_1,t_2,\cdots,t_n)$ 又记作 $P(G;t_1,t_2,\cdots t_n)$等.

定理 9.8.2 对称群 S_n 的循环指标为

$$Z(S_n;t_1;t_2;\cdots,t_n) = \sum_{(\lambda)} \frac{1}{1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\lambda_1!\lambda_2!\cdots\lambda_n!} t_1^{\lambda_1} t_2^{\lambda_2}\cdots t_n^{\lambda_n},$$

其中和式 $\sum_{(\lambda)}$ 指对方程 $1\cdot\lambda_1+2\cdot\lambda_2+\cdots+n\cdot\lambda_n=n$ 的所有非负整数解 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 求和.

定理 9.8.3 交错群 A_n 的轮换指标为

$$Z(A_n;t_1,\cdots,t_n) = \sum_{(\lambda)} \frac{2}{1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\lambda_1!\lambda_2!\cdots\lambda_n!} t_1^{\lambda_1}\cdots t_n^{\lambda_n},$$

其中和式 $\sum_{(\lambda)}$ 是对以下方程的所有非负整数解 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 求和.

$$\begin{cases} 1\cdot\lambda_1+2\cdot\lambda_2+\cdots+n\cdot\lambda_n=n, \\ \lambda_2+\lambda_4+\cdots=\text{偶数}. \end{cases}$$

定理 9.8.4 循环群 C_n 的轮换指标为

$$Z(C_n;t_1,\cdots,t_n)=\frac{1}{n}\sum_{k|n}\varphi(k)t_k^{\frac{n}{k}},$$

其中 $\varphi(k)$是欧拉 φ-函数(见例 9.2.5).

定理 9.8.5 二面体群 D_n 的轮换指标为

$$Z(D_n;t_1,\cdots,t_n)=\frac{1}{2}\{Z(C_n;t_1,\cdots,t_n)+\alpha_n\},$$

其中

$$\alpha_n=\begin{cases}t_1t_2^{\frac{n-1}{2}}, & n=\text{奇数},\\ \frac{1}{2}(t_2^{\frac{n}{2}}+t_1^2t_2^{\frac{n-2}{2}}), & n=\text{偶数}.\end{cases}$$

定理 9.8.6 设 $X=\{1,2,\cdots,n\}$,S_n 是 X 上的对称群,令 $X^{(2)}$ 为 X 上的二元子集(无序),$X^{(2)}=\{\{a,b\}\mid a,b\in X\}$. S_n 在 $X^{(2)}$ 上对应的置换群,记作 $S_n^{(2)}$,具体定义如下:$\forall g\in S_n$,有 $\sigma_g\in S_n^{(2)}$:$\sigma_g(\{i,j\})=\{g(i),g(j)\}$. 虽然 $S_n^{(2)}\cong S_n$,但因目标集不同,轮换指标也不同.

$S_n^{(2)}$ 的轮换指标为

$$Z(S_n^{(2)};t_1,\cdots,t_{\binom{n}{2}})=\sum_{(\lambda)}\frac{1}{1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\lambda_1!\lambda_2!\cdots\lambda_n!}$$

$$\cdot\Big(\prod_{k\geqslant 0}t_{2k+1}^{k\lambda_{2k+1}}\Big)\Big(\prod_{k\geqslant 1}(t_kt_{2k}^{k-1})^{\lambda_{2k}}t_k^{k\binom{\lambda_k}{2}}\Big)\Big(\prod_{k<l}t_{[k,l]}^{(k,l)\lambda_k\lambda_l}\Big).$$

其中和式 $\sum\limits_{(\lambda)}$ 是对 $1\cdot\lambda_1+2\cdot\lambda_2+\cdots+n\cdot\lambda_n=n$ 的所有非负整数解求和,(k,l) 和$[k,l]$ 分别表示 k 与 l 的最大公因子和最小公倍数.

定理 9.8.7 (群的简单积的轮换指标) 设 G 是集合 $X=\{x_1,x_2,\cdots,x_n,\}$上的置换群,$H$ 是 $Y=\{y_1,y_2,\cdots,y_m\}$上的置换群,令

$$G\cdot H=\{(g,h)\mid g\in G,h\in H\},W=X\cup Y.$$

定义 $G \cdot H$ 对 W 的作用为

$$(g,h)z = \begin{cases} g(z), 当\ z \in X, \\ h(z), 当\ z \in Y. \end{cases}$$

则 $G \cdot H$ 的轮换指标为

$$Z(G \cdot H;t_1,\cdots) = P(G;t_1,\cdots,t_n) \cdot P(H;t_1,\cdots,t_m).$$

定理 9.8.8 （群的笛卡儿积的轮换指标） 设 G 是 $X=\{x_1, x_2,\cdots,x_n\}$ 上的置换群，H 是 $Y=\{y_1,y_2,\cdots,y_m\}$ 上的置换群，定义 $G\times H$ 对 $X\times Y$ 的作用为

$$(g,h)(x,y) = (g(x),h(y)),$$

则 $G\times H$ 的轮换指标为

$$Z(G \times H;t_1,\cdots) = \frac{1}{|G|\cdot|H|}\sum_{\substack{g\in G\\ h\in H}}\prod_{\substack{1\leqslant k\leqslant n\\ 1\leqslant l\leqslant m}} t_{[k,l]}^{(k,l)\lambda_k(g)\mu_l(h)},$$

其中 $\lambda_k(g)$ 与 $\mu_l(h)$ 分别表示 g 与 h 的类型分别为 $1^{\lambda_1(g)}2^{\lambda_2(g)}\cdots n^{\lambda_n(g)}$ 与 $1^{\mu_1(h)}2^{\mu_2(h)}\cdots n^{\mu_n'(h)}$.

定理 9.8.9 （群的花环积的轮换指标） G 为 X 上的置换群，H 为 Y 上的置换群，令

$$G \otimes H = \{(g;h_1,h_2,\cdots,h_n) \mid g \in G, h_i \in H\},$$

定义 $G\otimes H$ 对 $X\times Y$ 的作用为

$$(g;h_1,\cdots,h_2)(x_i,y) = (g(x_i),h_i(y)),$$

则 $G\otimes H$ 的轮换指标为

$$Z(G \otimes H;t_1,\cdots) = Z(G,Z_1(H),Z_2(H),\cdots,Z_n(H)),$$

其中 $Z_k(H)=Z(H;t_k,t_{2k},\cdots,t_{mk}),k=1,2,\cdots,n.$

定理 9.8.10 （幂群的轮换指标） 设 G 是 X 上的置换群，H 是 Y 上的置换群，令

$$H^G = G \times H,$$

Y^X 为所有 X 到 Y 的映射的集合，定义 H^G 对 Y^X 的作用为

$$(g,h) \cdot f = hfg,$$

则 H^G 的轮换指标为

$$Z(H^G;t_1,\cdots)=\frac{1}{|G|\cdot|H|}\sum_{\substack{g\in G\\h\in H}}\prod_{k\geqslant 1}t_k^{\lambda_k(g,h)},$$

其中
$$\lambda_1(g,h)=\prod_{k\geqslant 1}\sum_{r|k}[r\lambda_r(h)]^{\lambda_k(g)},$$

$$\lambda_k(g,h)=\frac{1}{k}\sum_{r|k}\mu(r,k)\lambda_1(g^r,h^r),$$

其中 $\mu(r,k)$ 为因子格的 Möbius 函数(见 12.4 节).

9.9 Pólya 定理

定义 9.9.1 设 G 是集合 $X=\{1,2,\cdots,n\}$ 上的一个置换群, $A=\{a_1,a_2,\cdots,a_n\}$, $\Omega=A^X$ 为全体 X 到 A 的映射. 定义 G 对 Ω 的作用为: $\forall g\in G, f\in\Omega$ 有

$$g(f)=fg^{-1}①.$$

则每一个轨道

$$\Omega_f=\bar{f}=\{g(f)\mid g\in G\}$$

称为一个**映射格式**(function or mapping scheme)代表了映射的一个等价类, f 是这个格式的代表元.

定理 9.9.2 Pólya 定理 该定理是映射格式数的计数定理.

设 G 是 $X=\{1,2,\cdots,n\}$ 上的一个置换群, $A=\{a_1,a_2,\cdots,a_m\}$, G 对 A^X 的作用为: $g(f)=fg^{-1}$, $\forall f\in A^X$, 则 A^X 在 G 作用下的映射格式数为

$$Z(G;m,m,\cdots,m).$$

---

① 更直观地看: 设 $f=\begin{pmatrix}1 & 2 & \cdots & n\\ a_{i_1} & a_{i_2} & \cdots & a_{i_n}\end{pmatrix}$, 则

$$g(f)=\begin{pmatrix}g(1) & g(2) & \cdots & g(n)\\ a_{i_1} & a_{i_2} & \cdots & a_{i_n}\end{pmatrix}=f_1$$

f_1 与 f 的差别只是点号作了一个置换.

即把 m 代入 G 的轮换指标中各变量 t_i 所得之值.

Pólya 定理的魅力在于把一个十分复杂的求等价类数目的问题与方法表述得十分简单.

下面给出映射格式的生成函数的定义. 首先对集合 A 的元素定义权：$w(a_j)=w_j, j=1,2,\cdots,m$. 然后对每一个映射定义权：

$$w(f)=\prod_{i=1}^{n} f(i)=w_1^{r_1}w_2^{r_2}\cdots w_m^{r_m}, r_1+r_2+\cdots+r_m=n.$$

由于同一格式中的映射的权都相同,所以可定义映射格式的权：$w(\overline{f})=w(f)$.

定义 9.9.3 如果权为 $w_1^{r_1}w_2^{r_2}\cdots w_m^{r_m}$ 的映射格式数为 $C_{r_1r_2\cdots r_m}$,则函数

$$F(w_1,w_2,\cdots,w_m)=\sum_{\sum_{k=1}^{m} r_k=n} C_{r_1r_2\cdots r_m} w_1^{r_1}w_2^{r_2}\cdots w_m^{r_m}$$

称为映射格式的**生成函数**(generating function)或**计数函数**(enumeration function).

对于 X 中的任一元素 i, $w(f(i))$ 可能为 w_1,或 w_2,$\cdots$,或 w_m,令

$$h(w)=w_1+w_2+\cdots+w_m,$$

称为元素生成函数或元素计数函数.

定理 9.9.4 Pólya 定理 (映射格式数分类计数函数) 设 G 为 X 上的置换群, $A=\{a_1,a_2,\cdots,a_m\}$, G 对 A^X 的作用为 $g(f)=fg^{-1}$,则映射格式计数函数为

$$F(w_1,w_2,\cdots,w_m)=Z(G;h(w)).$$

其中 $h(w)=w_1+w_2+\cdots+w_m$, $Z(G;h(w))=Z(G;h(w),h(w^2),\cdots,h(w^n))$,即在 G 的轮换指标表达式中,变量 t_k 用 $h(w^k)$ 代替,$k=1,2,\cdots,n$.

该定理实际上是一个非常复杂的定理,但最后可用一个非常

简洁的式子 $Z(G;h(w))$ 表达，并且有非常便于记忆的方法：映射格式生成函数可由将元素生成函数 $h(w)$ 代入 G 的循环指标而得到.

由于 $G,X,A,h(w)$ 的不同，Pólya 定理可应用于不同的问题.

定理 9.9.5　de Bruijn 定理(对某个 A 上的置换不变的映射格式数)　设 X 上的置换群 G 作用于 A^X 上：$g(f)=fg^{-1}$，$g\in G$，$f\in A^X$. $\overline{f}$ 为一个映射格式. 现取 A 上的某个置换 σ，定义 σ 对 $\overline{f}$ 的作用为：$\sigma(\overline{f})=\overline{\sigma(f)}$. 若 $\sigma(\overline{f})=\overline{f}$，则称 σ 对 $\overline{f}$ 不变. 在所有映射格式中对 σ 不变的格式数的计数函数为

$$Z(G;p_1,p_2,\cdots p_n),$$

其中

$$p_k=\sum_{\substack{\sigma^k(a)=a\\ a\in A}} w(a)w(\sigma(a))\cdots w(\sigma^{k-1}(a)),$$

$k=1,2,\cdots,n$. 且当 $\{a\mid\sigma^k(a)=a\}=\varnothing$ 时 $p_k=0$.

9.10　Pólya 定理的应用

9.10.1　着色问题

设 $X=\{1,2,\cdots,n\}$ 代表 n 个点，G 为 X 上的一个置换群，$A=\{a_1,a_2,\cdots,a_m\}$ 为颜色集合，则 A^X 为 X 上的所有着色集合，$\overline{f}$ 称为一个着色格式，则由 Pólya 定理可求出着色格式数或着色格式数的计数函数.

例 9.10.1　用 m 种颜色对正六面体的顶点着色，求本质上不同的着色方法数及其生成函数.（本质上不同指在旋转群作用下不在同一轨道上的着色方法，即不同的着色格式.）

解　令 $X=\{1,2,3,4,5,6,7,8\}$ 为正六面体的顶点集合，$A=$

$\{a_1, a_2, \cdots, a_m\}$为 m 种颜色的集合. $G=\{(1234)(5678), \cdots\}$为该正六面体的旋转群,共有 24 个元素. 首先求出 G 的循环指标,可得

$$Z(G;t_1, \cdots, t_8) = \frac{1}{24}(t_1^8 + 8t_1^2 t_3^2 + 9t_2^4 + 6t_4^2).$$

于是由定理 9.9.2 得本质上不同的着色方法数为 $Z(G, m, \cdots, m) = \frac{1}{24}(m^8 + 17m^4 + 6m^2)$.

由定理 9.9.4 得着色格式的计数函数为

$$\begin{aligned} F_{\text{立方体}}(w_1, \cdots, w_m) &= Z(G;h(w)) \\ &= \frac{1}{24}\{(w_1 + \cdots + w_m)^8 + 8(w_1 + \cdots + w_m)^2(w_1^3 + \cdots + w_m^3)^2 \\ &\quad + 9(w_1^2 + w_2^2 + \cdots + w_m^2)^4 + 6(w_1^4 + \cdots + w_m^4)^2\}. \end{aligned}$$

当 m 是具体数时,很易得到:

$$\sum C_{k_1 k_2 \cdots k_m} w_1^{k_1} w_2^{k_2} \cdots w_m^{k_m}.$$

类似可求正 n 面体的顶点着色问题或面着色问题. 还可解决化学分子结构的计数问题,把不同的原子对应于颜色,例如苯环上结合不同原子得到的化合物数,就是对正六边形的顶点的着色问题.

例 9.10.2 用 6 种颜色 $a_1, a_1', a_2, a_2', a_3, a_3'$ 对正六面体的 6 个面着色,这时 $A = \{a_1, a_1', a_2, a_2', a_3, a_3'\}$,取 A 上的一个置换 $h = (a_1, a_1')(a_2, a_2')(a_3, a_3')$,求对 h 不变的着色格式数.

解 这时 $X = \{1,2,3,4,5,6\}$ 代表六个面,旋转群 $G = \{(1), (1234), \cdots\}$仍为 24 个元素,但表达形式与例 9.10.1 不同,可得轮换指标为

$$Z(G;t_1, \cdots, t_6) = \frac{1}{24}(t_1^6 + 3t_1^2 t_2^2 + 6t_1^2 t_4 + 6t_2^3 + 8t_3^2).$$

设权函数 $w(a_i) = w_i, w(a_i') = w_i', i = 1,2,3$. 由定理 9.9.5,需计

算 p_i：

$$p_1=0, p_2=2w_1w_1'+2w_2w_2'+2w_3w_3', p_3=p_5=0,$$

由于 p_4, p_6 在计算中不出现，可以不算，于是得对 h 不变的着色函数为

$$F(w_1, w_1', \cdots)=Z(G; p_1, \cdots, p_6)=\frac{1}{24}\cdot 6p_2^2$$

$$=2(w_1w_1'+w_2w_2'+w_3w_3')^3.$$

总格式数为 $F(1,1,\cdots)=2\cdot 3^3=54$.

如要求每种颜色都用到的格式数，即为 $w_1w_1'w_2w_2'w_3w_3'$ 项的系数，由上式可得 $2\cdot\frac{3!}{1!1!1!}=12$.

表 9.2 列出正多面体顶点着色格式数.

表 9.2　正多面体顶点着色格式数

正多面体	顶点数	边数	面数	面形	旋转群，阶	着色格式数（n 为颜色数）
正四面体	4	6	4	正三角形	A_4, 12	$\frac{1}{12}(n^4+11n^2)$
正六面体	8	12	6	正方形	S_4, 24	$\frac{1}{24}(n^8+17n^4+6n^2)$
正八面体	6	12	8	正三角形	S_4, 24	$\frac{1}{24}(n^6+3n^4+12n^3+8n^2)$
正十二面体	20	30	12	正五边形	A_5, 60	$\frac{1}{60}(n^{20}+15n^{10}+20n^8+24n^4)$
正二十面体	12	30	20	正三角形	A_5, 60	$\frac{1}{60}(n^{12}+15n^6+44n^4)$

9.10.2　布置问题

将一些物体放入一些房间的问题可以与映射格式问题类似地来讨论.

例 9.10.3 将 4 个物体$\{B,B,C,C\}$放入两个房间$\{a,b\}$内，问有多少种放法(允许一个房间为空)?

解 令 $X=\{1,2,3,4\}$，其中 1，2 代表物体 B，3，4 代表物体 C，$A=\{a,b\}$，每一个布置对应一个映射 $f:x\to A$.

令 $G=\{(1),(12),(34),(12)(34)\}$是 X 上的一个置换群，则原问题的布置数就是 G 作用于 A^X 的映射格式数，可用 Pólay 定理求得. G 的轮换指标为

$$Z(G;t_1,t_2,t_3,t_4)=\frac{1}{4}(t_1^4+2t_1^2t_2+t_2^2),$$

则布置数为

$$N=Z(G;2,2,2,2)=9.$$

计数函数为

$$\begin{aligned}F(w_1,w_2)&=\frac{1}{4}\{(w_1+w_2)^4+2(w_1+w_2)^2(w_1^2+w_2^2)\\&\quad+(w_1^2+w_2^2)^2\}\\&=w_1^4+2w_1^3w_2+3w_1^2w_2^2+2w_1w_2^3+w_2^4.\end{aligned}$$

取 $\sigma=(a,b)$，则对 σ 不变的布置格式计数函数为：$p_1=0$，$p_2=2w_1w_2$，由定理 9.9.5 得.

$$F_\sigma(w_1,w_2)=w_1^2w_2^2,$$

即只有一个布置格式满足对 σ 不变，即 $BC|BC$

如果不考虑房间 a 与 b 的区别，问这样的布置方法数是多少?设全部布置格式的集合为 Ω，$\{a,b\}$上的置换群为 $H=\{(1),(a,b)\}$，H 对 Ω 的作用为 $h(\overline{f})=\overline{hf}$，这时可用 Burnside 引理来求该数. 单位元(1)的不动点数为$|\Omega|=9$，(a,b)的不动点数为 1，故

$$N=\frac{1}{|H|}\sum_{h\in H}x(h)=\frac{1}{2}(9+1)=5.$$

这 5 种布置方法为：$|BBCC$，$B|BCC$，$C|BBC$，$BB|CC$，$BC|BC$.

9.10.3 开关线路与布尔函数的计数问题

n个开关组成的开关线路对应一个n元布尔函数：$f(x_1,x_2,\cdots,x_n)$：$\{0,1\}^n\rightarrow\{0,1\}$. 可以通过计算布尔函数的数目来计数不同的开关线路的数目，下面分几种情形计算布尔函数的数目.

(1) 全部布尔函数数目　设$A=\{0,1\}$，$X=A^n$，则全部布尔函数的集合为A^X，所以全部布尔函数的数目为$|A^X|=2^{2^n}$. 但如果两个函数仅仅是自变量的次序不同，则认为这两个函数是等价的，因此，等价类的数目就是A^X在S_n作用下的函数格式数.

(2) 在S_n作用下的格式数　令$G=S_n$，定义G对$\Omega=A^X$的作用为：$\sigma\in S_n$，$f\in A^X$，$\sigma(f)=f(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)})$，则$\Omega$在$S_n$作用下的格式数为

$$Z(S_n;2,\cdots,2).$$

(3) 在$C_2^n\times S_n$作用下的格式数　如果考虑自变量x_i的两个取值0,1可交换，即两个函数f_1与f_2，只要把f_1的自变量取值中，0与1互换，就变成f_2，则认为它们是等价的，同时考虑(2)中的自变量次序的置换，可令

$$G=C_2^n\times S_n=\{(\pi,\sigma)\mid\pi\in C_2^n,\sigma\in S_n\},$$

定义G对$\Omega=A^X$的作用为

$$(\pi,\sigma)f(x_1,x_2,\cdots,x_n)=f(\pi x_{\sigma(1)},\pi x_{\sigma(2)},\cdots,\pi x_{\sigma(n)}),$$

则Ω在G作用下的函数格式数为

$$Z(G;2,2,\cdots,2).$$

(4) 考虑变量次序的置换及自变量与因变量值的对换的函数格式数　如果除了考虑(2)与(3)的分类外，当一个函数f_1的函数值中0与1互换时变成了函数f_2，就认为f_1与f_2等价，由此得到的等价类数目可进一步减少.

对n从1到5所得结果列于表9.3. $n=1$时布尔函数及函数

格式见表 9.4.

表 9.3 不同类型的布尔函数数目

n	1	2	3	4	5
全部布尔函数数	$2^{2^1}=4$	$2^{2^2}=16$	$2^{2^3}=256$	$2^{2^4}=65536$	$2^{2^5}=4294967296$
在 S_n 作用下的函数格式数	4	12	80	3984	37333248
在 $C_2^n\times S_n$ 作用下的函数格式数	3	6	22	402	1228158
在 $C_2^n\times S_n$ 作用下且考虑因变量值 0,1 互换的等价类数	2	4	14	222	616126

表 9.4 $n=1$ 时布尔函数及函数格式

	f_1	f_2	f_3	f_4
全部布尔函数	x , $f_1(x)$ 0 , 0 1 , 0	x , $f_2(x)$ 0 , 0 1 , 1	x , $f_3(x)$ 0 , 1 1 , 0	x , $f_4(x)$ 0 , 1 1 , 1
在 S_n 作用下的函数格式	$\bar{f}_1$	$\bar{f}_2$	$\bar{f}_3$	$\bar{f}_4$
在 $C_2\times S_n$ 作用下的函数格式	$\bar{f}_1$	$\bar{f}_2=\bar{f}_3$		$\bar{f}_4$
在 $C_2\times S_n$ 作用下且因变量 0,1 互换的函数格式	$\bar{f}_1=\bar{f}_4$	$\bar{f}_2=\bar{f}_3$		

9.10.4 图的计数问题

用 Pólya 计数理论可解决不同构的图的计数问题. 设 $V=\{1,2,\cdots,n\}$为顶点集合,$X=V$ 的二元子集$=\{\{i,j\}\mid_{i,j\in V且i\neq j}\}$,$A=\{0,1\}$,则 $f=X\to A$ 对应一个图 $G=(V,E)$,当 $f(\{i,j\})=1$ 时$\{i,j\}\in E$,否则$\{i,j\}\notin E$. 设 G 是 X 上的一个置换群,定义 G 对 A^X 的作用为

$$g(f)\{i,j\} = f(\{g(i),g(j)\}),$$

则 A^X 在 G 作用下的不同图类可用 Pólya 计数理论求得(见 9.11 节).

9.11 图的计数

一个图 $G=(V,E)$的点集 V 中的每个点是带标号的,称此图为**有标号图**(labeled graph). 如果把互相同构的图(同构概念见 10.8 节)看作是相同的,则每一个同构类称为一个**无标号图**(unlabeled graph).

因此,图的计数问题通常分为有标号图的计数和无标号图的计数.

定义 9.11.1 设点数为 n,边数为 m 的某类图的个数为 $C_{n,m}$,则以下的形式级数

$$F(x,y) = \sum C_{n,m}x^n y^m,$$

称为该类图的**生成函数或计数函数**.

当 n 固定时,生成函数可表为

$$F_n(y) = \sum C_m y^m,$$

其中 C_m 为边数为 m 的该类图的数目.

当只考虑点数时,生成函数可表为

$$F(x) = \sum C_n x^n,$$

其中 C_n 为 n 阶该类图的数目.

定理 9.11.2 （有标号简单图的计数） n 阶有标号简单图的生成函数为

$$G_n(y) = (1+y)^{\binom{n}{2}},$$

总数为

$$G_n(1) = 2^{\binom{n}{2}}.$$

定理 9.11.3 （与某个图同构的有标号图的数目） 设 $G=(V,E)$ 为已知的一个图,$\Gamma(G)$ 为 G 的自同构群（见 10.8 节）,则与 G 同构的所有有标号简单图的数目为

$$\frac{n!}{|\Gamma(G)|}.$$

定理 9.11.4 Cayley 定理 （树（有标号）的数目） n 阶树的数目为 n^{n-2}.

定理 9.11.5 （无标号有根树的计数） 设 $T(x)$ 是无标号有根树的生成函数,则 $T(x)$ 满足以下方程

$$T(x) = x\exp\left\{\sum_{k=1}^{\infty}[T(x^k)/k]\right\}.$$

且可算得

$$T(x) = x + x^2 + 2x^3 + 4x^4 + 9x^5 + 20x^6 + 48x^7 + 115x^8 + 286x^9 + 719x^{10} + \cdots$$

设 T_n 是 n 阶有根树的数目,则 T_n 有以下递推公式

$$T_{n+1} = n^{-1}\sum_{k=1}^{n}\left(\sum_{d|k} dT_d\right)T_{n-k+1}.$$

定理 9.11.6 （无标号树的计数） 设 $t(x)$ 为无标号树的计数函数,$T(x)$ 为无标号有根树的计数函数,则有以下关系

$$t(x) = T(x) - \frac{1}{2}\{T^2(x) - T(x^2)\},$$

且有

$$t(x)=x+x^2+x^3+2x^4+3x^5+6x^6+11x^7+23x^8+47x^9+106x^{10}+\cdots$$

定理 9.11.7 （无标号简单图的计数） 设 $S_n^{(2)}$ 为对称群 S_n 在$[1,n]$的二元子集上对应的群(见定理 9.8.6)，则 n 阶无标号简单图的生成函数为

$$\begin{aligned}F_n(y)&=Z(S_n^{(2)};1+y)\\&=\sum_{(\lambda)}\frac{1}{1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\lambda_1!\lambda_2!\cdots\lambda_n!}\\&\quad\cdot\Big(\prod_{k\geqslant 1}(1+y^k)^{k\binom{\lambda_k}{2}}\Big)\Big(\prod_{r\geqslant 0}(1+y^{2r+1})^{r\lambda_{2r+1}}\Big)\\&\quad\cdot\Big(\prod_{r\geqslant 1}(1+y^r)^{\lambda_{2r}}(1+y^{2r})^{(r-1)\lambda_{2r}}\Big)\Big(\prod_{k>l}(1+y^{[k,l]})^{(k,l)\lambda_k\lambda_l}\Big),\end{aligned}$$

其中 $\sum_{(\lambda)}$ 为对满足方程 $1\cdot\lambda_1+2\cdot\lambda_2+\cdots+n\cdot\lambda_n=n$ 的所有非负整数解求和(具体数目见表 9.5).

定理 9.11.8 （连通图的计数） 设 $g(x)$ 是某类无标号图的计数函数，$C(x)$ 是该类无标号连通图的计数函数，且 $g(x)=\sum_{n=1}^{\infty}g_nx^n$，$C(x)=\sum_{n=1}^{\infty}C_nx^n$，则有

(1) $1+g(x)=\exp\sum_{k=1}^{\infty}(C(x^k)/k)$.

(2) $na_n-ng_n=\sum_{k=1}^{n-1}ka_kg_{n-k}$，

$$C_n=\sum_{d\mid n}\frac{1}{d}\mu(d)a_{\frac{n}{d}}.$$

其中 a_k 满足 $\log(1+g(x))=\sum_{k=1}^{\infty}a_kx^k$，$\mu(d)$ 为 Möbius 函数(参见 12.4 节).

定义 9.11.9 （自补图的计数） 设 $G=(V,E)$，令 $\overline{G}=(V,\overline{E})$，

其中 $\overline{E}=E(K_n)\backslash E$，称 $\overline{G}$ 为 G 的补图. 若 $G\cong\overline{G}$,，则称 G 是**自补图**(self-complementary graph). 它对应于集合 A^X 的映射格式对颜色对换 $\sigma=(0,1)$ 不变的映射格式数，可用定理 9.9.5 求得，为

$$P(S_n^{(2)};0,2,0,2,\cdots),$$

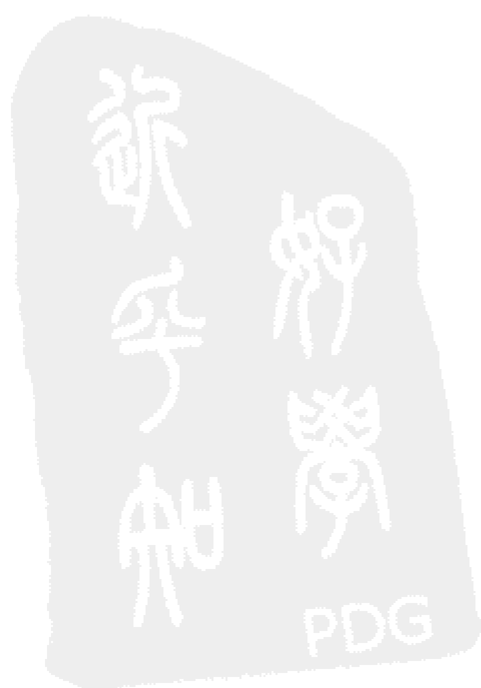
自补图的计数函数为

$$P(S_n^{(2)};0,2w,0,2w,\cdots).$$

具体数目见表 9.5.

表 9.5　某些无标号图的数目

点数 n	树	图	连通图	自补图	Hamilton 图	外平面图
1	1	1	1	1		
2	1	2	1	0		
3	1	4	2	0	1	1
4	2	11	6	1	3	2
5	3	34	21	2	8	3
6	6	156	112	0	48	9
7	11	1044	853	0	383	20
8	23	12346	11117	10	6196	75
9	47	274668	261080	36		262
10	106	12005168	11716571	0		1 117



10 图的基本概念与参数

10.1 图的定义与简单分类

定义 10.1.1 图(graph)$G=(V,E)$是由集合 V 和集合 E 构成的有序对,其中 $V=\{v_1,v_2,\cdots,v_n\}$称为(**顶**)**点集**(vertex set),$E=\{e_1,e_2,\cdots,e_m\}$是由 $V\times V$ 的元素组成的可重集合,称为**弧集**(arc set). 点集又记成 $V(G)$,弧集又记成 $E(G)$.

当$|V(G)|=n$时,称 G 的**阶**(order)为 n,又记成$|G|=n$,若$|V(G)|=n$,$|E(G)|=m$,则称 G 为一个(n,m)阶图.

定义 10.1.2 若 $E(G)$是一个多重集合,则称 G 是一个**多重图**(multigraph);若 $E(G)$中元素重复出现的次数最多为 p 次,则称 G 为 ***p*-图**.

定义 10.1.3 若对 $E(G)$中的元素规定$(v_i,v_j)=(v_j,v_i)$,则称 G 为**无向图**(undirected graph),否则称 G 为**有向图**(digraph). 对无向图 G,集合 $E(G)$称为**边集**(edge set). 有向图通常记作:$D=(V,A)$,其中 A 为 G 的弧集,又记作 $A(G)$.

定义 10.1.4 元素$(v_i,v_i)\in E(G)$,即两个端点相同的弧或边称为一个**环**(loop).

定义 10.1.5 无环的 1-图称为**简单图**(simple graph),特别是无向的无环的 1-图,通常简称为图.

定义 10.1.6 只有一个点的图,称为**平凡图**(trivial graph).

定义 10.1.7 $E(G)=\varnothing$的图称为**空图**(empty graph).

定义 10.1.8 $\forall v_i,v_j\in V(G)(i\neq j)$,均有$(v_i,v_j)\in E(G)$的简单图称为**完全图**(complete graph),n 阶无向完全图记作 K_n.

定义 10.1.9 设 $V=X\cup Y$ 且 $X\cap Y=\varnothing$，$\forall(v_i,v_j)\in E$ 有 $v_i\in X,v_j\in Y$ 或 $v_i\in Y,v_j\in X$，则称 G 是一个**二分图**或二部图(bipartite graph)，记作 $G=(X,Y,E)$.

定义 10.1.10 设无向二分图 $G=(X,Y,E)$ 满足 $|X|=n$，$|Y|=m$，$\forall u\in X,v\in Y$ 有 $(u,v)\in E$，称为**完全二分图**(complete bipartite graph)，记作 $K_{n,m}$.

定理 10.1.11 二分图的性质 G 是二分图的充分必要条件是 G 不包含奇圈.

定义 10.1.12 设 $V(G)=V_1\cup V_2\cup\cdots\cup V_k$，$V_i\cap V_j=\varnothing(i\neq j)$，在同一个 V_i 内的点之间无边相联，则称 G 为 **k-分图**(k-partite graph).

定义 10.1.13 **完全 k-分图**(complete k-partite graph) $K_{n_1,n_2,\cdots,n_k}$ 的定义与完全二分图类似.

定义 10.1.14 每个点的次数都是 k 的图，称为 **k-正则图**(regular graph).

定义 10.1.15 无圈的连通图称为**树**(tree).

定理 10.1.16 树的等价条件 设 $G=(V,E)$ 是一个简单图，$p=|V|$，$q=|E|$，则以下命题等价：

(1) G 是一个树.

(2) G 的任意两个点由唯一的一条路联结.

(3) G 是连通的，且 $q=p-1$.

(4) G 是无圈的，且 $q=p-1$.

(5) G 是无圈的，且 $\forall e=(v_i,v_j)\notin E$ 则 $G+e$ 恰有一个圈.

定义 10.1.17 图 G 的每一个连通分支都是树，则称 G 是**森林**(forest).

定义 10.1.18 设 G 是一个无向图，若对 G 的每一条边规定一个方向，由此得到的有向图 D 称为 G 的一个**定向**(orientation)，G 称为 D 的**基图**(underlying graph).

定义 10.1.19 K_n 的一个定向称为**竞赛图**(tournament).

定义 10.1.20 有欧拉闭迹的图称为**欧拉图**(Euler graph).

定义 10.1.21 有哈密尔顿圈的图称为**哈密尔顿图**(Hamiltonian graph).

定义 10.1.22 设 $G=(V,E)$ 是一个简单图,若 G 与它的补图 G^c(定义见 9.11.9)同构,则称 G 为**自补图**(selfcomplementary graph).

定义 10.1.23 设 $G(V,E)$,G 的**线图**(line graph)$L(G)$ 定义为:$L(G)$ 为点集为 G 的边集,$L(G)$ 中两点相邻当且仅当 G 中两边相邻.

定义 10.1.24 图 G 的**全图**(total graph)$T(G)$ 定义如下:$T(G)$ 为点集是 $V(G)\cup E(G)$,$\Gamma(G)$ 中两点相邻当且仅当它们在 G 中相邻或相关联.

10.2 邻接与关联

定义 10.2.1 若 $e=(v_i,v_j)\in E(G)$,则称 v_i 和 v_j 是 e 的**端点**(endpoint);若 e 是有向图中的弧,则称 v_i 是 e 的**始端**(initial endpoint),v_j 是 e 的**终端**(terminal endpoint),e 是 v_i 的**出弧**(outarc),e 是 v_j 的**入弧**(inarc).

定义 10.2.2 若 $e=(v_i,v_j)\in E(G)$,则称 v_i 与 v_j **相邻**或**邻接**(adjacent),e 与 v_i、v_j **关联**(incident).当两条边有公共端点时,称它们相邻或邻接.

定义 10.2.3 在图 G 中与 v 相邻的点的集合称为**邻集** $N_G(v)$.若 G 是有向图,则 $N_G^-(v)=\{u\in V\mid(u,v)\in A(G)\}$ 称为 v 的**内邻集**(inner neighbour set);$N_G^+(v)=\{u\in V\mid(v,u)\in A(G)\}$,称为 v 的**外邻集**(outer neighbour set).$N_G(v)=N_G^-(v)\cup N_G^+(v)$.

定义 10.2.4 设 $G=(V,E)$是简单图,则

$$\mathbf{A}=(a_{ij})_{n\times n},\quad a_{ij}=\begin{cases}1, & \text{当}(v_i,v_j)\in E;\\ 0, & \text{否则},\end{cases}$$

称为 G 的**邻接矩阵**(adjacent matrix). 类似可定义 p 图的邻接矩阵,这时 a_{ij} 为 v_i 到 v_j 的弧的数目.

定义 10.2.5 设 $G=(V,E)$,$V=\{v_1,v_2,\cdots,v_n\}$,$E=\{e_1,e_2,\cdots,e_m\}$,则

$$\mathbf{C}=(c_{ij})_{n\times m},\quad c_{ij}=\begin{cases}1, & v_i\text{ 与 }e_j\text{ 关联};\\ 0, & \text{否则},\end{cases}$$

称为 G 的**关联矩阵**(incident matrix),记作 $\mathbf{C}(G)$.

10.3 度、度序列与边数

定义 10.3.1 设与 v 关联的边数(环算 2),称为 v 的**次**或**度**(degree),记作 $d(v)$. 若 G 为有向图,则 G 中以 v 为终点的弧数称为**入度**(indegree),记作 $d^-(v)$;以 v 为始端的弧数称为**出度**(outdegree),记作 $d^+(v)$.

定义 10.3.2 图 G 中的**最大度数**记作 $\Delta(G)$,**最小度数**记作 $\delta(G)$,这两个记号几乎在所有的图论文献中作为统一的专用符号.

定理 10.3.3 度的性质 对任何图 $G=(V,E)$,有

(1) $\sum\limits_{v\in V}d(v)=2|E|$;

(2) $\delta(G)=2\Rightarrow G$ 包含一个圈;

(3) 设 $|V|=n$,若 G 不含完全 k 子图,则有

$$\delta(G)\leqslant\left\lfloor\frac{(k-2)n}{k-1}\right\rfloor.$$

定义 10.3.4 设 $G=(V,E)$,$V=\{v_1,v_2,\cdots,v_n\}$,则序列

$$d_1(v_1),d_2(v_2),\cdots,d_n(v_n)$$

称为 G 的**度序列**(degree sequence).

设 $d=(d_1,d_2,\cdots,d_n)$ 是一个非负整数序列,若有一个图的度序列为 d,则称 d 为**图序列**(graph sequence).

整数序列是图序列的充要条件有以下定理.

定理 10.3.5 整数序列 $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_n (n>2)$ 是一个简单图的度序列的充要条件是同时满足以下条件:

(1) $d_n \geqslant 1$;

(2) $\sum_{i=1}^{n} d_i \geqslant 2(n-1)$;

(3) $\sum_{i=1}^{n} d_i$ 是偶数;

(4) $\sum_{i=1}^{k} d_i \leqslant \sum_{i=1}^{k} \overline{d}_i (k=1,2,\cdots,n)$,其中 $\overline{d}_i$ 是满足 $j<i$ 及 $d_j \geqslant i-1$ 的指标 j 的个数与满足 $j>i$ 及 $d_j>i$ 的指标 j 的个数之和.

定理 10.3.6 整数序列 $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_n (n>2)$ 是一个简单 2 连通图的度序列的充要条件是同时满足以下条件:

(1) $d_n \geqslant 2$;

(2) $\sum_{i=1}^{n} d_i \geqslant 2(n+d_1-2)$;

(3) $\sum_{i=1}^{n} d_i$ 是偶数;

(4) $\sum_{i=1}^{k} d_i \leqslant \sum_{i=1}^{k} \overline{d}_i (k=1,2,\cdots,n)$,其中 $\overline{d}_i$ 的意义同(定理 10.3.5)中的(4).

定理 10.3.7 不含$(m+1)$团的图的最大边数(Turan 定理)

设 G 是 n 阶图,不含$(m+1)$团,则有

$$|E(G)| \leqslant |E(T_{m,n})| = \binom{n}{2} - (q-1)\left(n-\frac{mq}{2}\right)$$

$$=\binom{n-k}{2}+(m-1)\binom{k+1}{2},$$

其中 $q=\lceil \frac{n}{m} \rceil, k=\lfloor \frac{n}{m} \rfloor$，当且仅当 $G\cong T_{m,n}$ 时等式成立，图 $T_{m,n}$ 的意义见定义 10.10.21.

定理 10.3.8 不含$(m+1)$独立集的图的最少边数(Turan 定理的另一形式)

设 G 是 n 阶图，不含$(m+1)$独立集，则有

$$|E(G)|\geqslant|E(T^c_{m,n})|=(q-1)\left(n-\frac{mq}{2}\right),$$

其中 q 的意义同定理 10.3.7，当且仅当 $G\cong T_{m,n}$ 时等式成立.

定理 10.3.9 Turan 定理的另一表达形式 设 $G=(V,E)$，$|V|=n$，不含 k-团，则有

$$|E|\leqslant\frac{k-2}{k-1}\frac{n^2-r^2}{2}+\binom{r}{2},$$

其中 r 是 n 被 $k-1$ 除所得之余数：$n=(k-1)t+r, 0\leqslant r<k-1$，且上式中之最大值可达到，达到此最大值的图在同构意义下唯一，为以下形式的完全 $k-1$ 分图：

$$K_{\underbrace{t,t,\cdots,t}_{k-1-r个},\underbrace{t+1,\cdots,t+1}_{r个}}.$$

特别是，当 G 中不含三角形时有 $|E|\leqslant\lfloor \frac{n^2}{4} \rfloor$.

定理 10.3.10 连通度为 m 的图的边数 设 $G=(V,E)$是连通度为 m 的 n 阶图，则有

$$|E|\geqslant\frac{mn}{2},$$

达到最少边的图 $H_{m,n}$ 的构造见定义 10.10.22.

10.4 子图

定义 10.4.1 设 $G=(V,E)$，$H=(V_1,E_1)$满足 $V_1\subseteq V$ 和

$E_1 \subseteq E$,则称 H 是 G 的**子图**(subgraph),G 是 H 的**扩图**(extension graph),记作 $H \subseteq G$.

定义 10.4.2 设 H,G 为两个图,若满足 $H \subseteq G$ 和 $V(H)=V(G)$,则称 H 是 G 的**生成子图**(spanning subgraph). 有些书中又称为**支撑子图**. 若 G 的生成子图是树,则称它是 G 的**生成树**(spanning tree).

定义 10.4.3 设 $G=(V,E)$,$V_1 \subseteq V$,$E_1 \subseteq E$,记 $E[V_1]$ 为 E 中两个端点均在 V_1 中的边的集合,$V[E_1]$ 为 E_1 中的边的端点集合,则称 $G[V_1]=(V_1,E[V_1])$ 为由 V_1 导出的**导出子图**(induced subgraph);$G[E_1]=(V[E_1],E_1)$ 为由 E_1 导出的子图.

10.5 路与圈

定义 10.5.1 图 G 中前后互相关联的点边序列:$W=v_0e_1v_1e_2v_2\cdots e_kv_k$ 称为一个**通道**(walk). 若 t 是 G 中一个通道,其中的边不重复,则称 t 是 G 中一条**迹**(trail). 迹所含的边数称为该迹的长度. 若 P 是 G 中一条迹且其中点不重复,则称 P 为 G 中一条路(path).

定义 10.5.2 G 中一条起点与终点相同的闭路 C 称为一个**圈**(cycle). 在有向图中若圈上的弧的方向保持一致,则称它为回路(circuit).

定义 10.5.3 图 G 中包含每一条边的迹称为**欧拉迹**(Euler trail). 包含每一个点的路(圈)称为**哈密尔顿路(圈)**(Hamiltonian path (cycle)). 有欧拉闭迹的图称为**欧拉图**,有哈密尔顿圈的图称为**哈密尔顿图**.

定理 10.5.4 设 G 是连通图,则图 G 中有欧拉迹的充分必要条件是 G 中奇次点的数目 $\leqslant 2$. G 中有欧拉闭迹的充分必要条件是 G 中无奇次点.

定义 10.5.5 设$G=(V,E)$,$E=\{e_1,e_2,\cdots,e_m\}$,C是G中一个圈,则向量

$$\alpha=(u_1,u_2,\cdots,u_m),$$

其中

$$u_i=\begin{cases}1, & \text{当 } e_i\in C\\ 0, & \text{否则}\end{cases}\quad (i=1,2,\cdots,m),$$

则称α为一个对应于C的**圈向量**(cycle vector).

定义 10.5.6 设$\alpha_1,\alpha_2,\cdots,\alpha_r$是图$G$的圈向量,满足(运算在域$(Z_2,+)$中进行):

(1) $\alpha_1,\alpha_2,\cdots,\alpha_r$线性无关,

(2) G中任一个圈向量α均可由$\alpha_1,\alpha_2,\cdots,\alpha_r$线性表出,则称$\alpha_1,\alpha_2,\cdots,\alpha_r$为$G$的一组**圈基**(cycle basis).

由圈基在Z_2^m中生成的线性子空间称为图G的**圈空间**(cycle space),圈空间中每一个向量是圈向量或一些圈向量之和.

定义 10.5.7 图G的圈空间的维数称为G的**圈秩**(cycle rank),记作$\gamma'(G)$,并满足以下等式:

$$\gamma'(G)=m-n+\omega(G),$$

其中$n=|V|$,$m=|E|$,$\omega(G)$为G的连通分支数目.

定义 10.5.8 图的**秩**(rank)定义为$r(G)=n-\omega(G)$.

10.6 距离与中心

定义 10.6.1 设u,v为图G中两点,则u与v之间的最短路的长度(路长指路中所含的边数)称为u与v之间的**距离**(distance),记作$d(u,v)$.

定义 10.6.2 设$G=(V,E)$,图G中两点之间距离的最大值,称为G的**直径**(diameter),记作$d(G)$,即

$$d(G)=\max_{u,v\in V} d(u,v).$$

设 $v\in V$，v 与其他各点距离的最大值，称为 v 的**离心率**(eccentricity)，记作 $\rho(v)$，即

$$\rho(v) = \max_{\substack{u\in V\\ u\neq v}}\{d(u,v)\}.$$

图 G 中的最小离心率，称为 G 的**半径**(radius)，记作 $r(G)$，即

$$r(G) = \min_{v\in V}\{\rho(v)\}.$$

因此，图 G 的半径不一定是图 G 的直径的二分之一.

定义 10.6.3 图 G 中离心率等于图的半径的点 v：$\rho(v)=r(G)$ 称为 G 的**中心点**. 中心点的集合称为 G 的**中心**(centre).

图 G 中最长圈的长度称为 G 的**周长**(circumference)，G 中最短圈的长度称为(**腰**)**围长**(girth).

10.7 图的运算

定义 10.7.1 设 $G=(V,E)$，$V'\subseteq V$，$E'\subseteq E$，则规定以下记号：

$G-V'=G[V\backslash V']$，即从 G 中去掉子集 V' 及与其关联的边.

$G-E'=G[E\backslash E']$，即从 G 中去掉边子集 E'.

若 $E_1\subseteq V\times V\backslash E$，则规定 $G+E_1=(V,E\cup E_1)$.

此外还规定：$G-v=G-\{v\}$，$G-e=G-\{e\}$.

定义 10.7.2 设 $G_1=(V_1,E_1)$，$G_2=(V_2,E_2)$ 为两个图，则

$$G_1\cup G_2=(V_1\cup V_2,E_1\cup E_2),$$
$$G_1\cap G_2=(V_1\cap V_2,E_1\cap E_2),$$

分别称为 G_1 与 G_2 的**并**(union)和**交**(intersection).

当 G_1 与 G_2 不相交时，它们的并记作 G_1+G_2.

定义 10.7.3 设 G_1 与 G_2 为两个图，将 G_1 的每一个点与 G_2 的每一个点用边相连，所得的图称为 G_1 与 G_2 的**联**(join)，记作 $G_1\vee G_2$.

定义 10.7.4 设 $G_1=(V_1,E_1)$， $G_2=(V_2,E_2)$，令

$V=V_1\times V_2$,

$E=\{((u,v_i),(u,v_j))\mid v_iv_j\in E_2\}\cup\{((u_k,v),(u_l,v))\mid u_ku_l\in E_1\}$

则**图的笛卡儿积**(cartesian product of graphs)为

$$G_1\times G_2=(V,E).$$

定义 10.7.5 设 $G=(V,E)$，令 $E^c=\{(u,v)\mid(u,v)\overline{\in}E\}$，则 $G^c=(V,E^c)$称为 G 的**补图**(complement).

定义 10.7.6 设 H 是 G 的子图，将 G 去掉 H 的边，所得之图，记作 $\overline{H}$，称为子图 H 的**余**(complement).

定义 10.7.7 设 $G=(V,E)$，**图的幂**(power) G^k 定义为：$V(G^k)=V$,

$E(G^k)=\{(u,v)\mid d_G(u,v)\leqslant k\}$，其中 $d_G(u,v)$表示 u,v 两点在 G 中之距离.

定义 10.7.8 设 $e\in E(G)$，将 e 收缩为一点，记作 $G\cdot e$. 令 $G'=G\cdot e$，称 G'为 G 的一次初等收缩，若 G_1 是 G 经过若干次初等收缩得到，则称 G 可收缩到 G_1，或 G_1 是 G 的**收缩**(contraction).

定义 10.7.9 设 $G_1=(V_1,E_1)$，$G_2=(V_2,E_2)$，则**图的合成或字典积**(composition or lexicographic product of graphs) $G_1[G_2]=(V,E)$，其中

$$V=V_1\times V_2, E=\{\{(u_1,u_2),(v_1,v_2)\}\mid(u_1,v_1)\in E_1 \text{ 或 } u_1=v_1 \text{ 且}(u_2,v_2)\in E_2\}.$$

定义 10.7.10 若在一个图 G 的一些边上加一些点，所得的图 G'称为 G 的**细分**(subdivision).

10.8 图的同构、同态与同胚

设 $G_1=(V_1,E_1)$，$G_2=(V_2,E_2)$为两个图.

定义 10.8.1 若存在双射 $f: V_1 \to V_2$ 满足

$$(v_1, v_2) \in E_1 \Leftrightarrow (f(v_1), f(v_2)) \in E_2,$$

则称 G_1 与 G_2 **同构**(isomorphic):记作 $G_1 \cong G_2$.

定义 10.8.2 设 $G=(V,E)$,若有双射 $f: V \to V$ 满足

$$(v_1, v_2) \in E_1 \Leftrightarrow (f(v_1), f(v_2)) \in E_2,$$

则称 f 是 G 上的一个**自同构**(automorphism).

G 上的所有自同构的集合记作 $\Gamma(G)$ 或者 $\mathrm{Aut}(G)$,对映射的复合构成一个群,标为 G 的**自同构群**(automorphism group),或简称为**图 G 的群.**

猜想 10.8.3 设 $G=(V,E)$, $H=(U,F)$ 为两个 n 阶图,若对每一个 $i(1 \leqslant i \leqslant n)$, $G_i = G - v_i$, $H_i = H - u_i$,有 $G_i \cong H_i$,则 $G \cong H$. 此猜想称为 **Ulam 猜想**也称为**重构猜想**(reconstruction conjecture),至今未解决.

定义 10.8.4 设 $G_1=(V_1,E_1)$, $G_2=(V_2,E_2)$ 为两个图,若存在映射 $f: V_1 \to V_2$ 满足

$$(v_1, v_2) \in E_1 \Rightarrow (f(v_1), f(v_2)) \in E_2,$$

则称 f 是 G_1 到 G_2 的一个**同态**(homomorphism).

定义 10.8.5 设 G_1 与 G_2 是通过对同一个图 G 的边细分而得到,所谓细分是在某些边上加一些点,则称 G_1 与 G_2 **同胚**(homemorphic).

10.9 图的独立集、团和覆盖

定义 10.9.1 设 $G=(V,E)$, $S \subseteq V$,若 S 内任何两点之间均无边相连,则 S 是 G 的一个**独立集**(indepedent set). G 中一个完全子图称为 G 中的一个**团**(clique). $M \subseteq E$,若 M 中的边互相不相邻,则称 M 是 G 中一个**边独立集**,又称**匹配**(matching).

定义 10.9.2 G 中最大独立集的基数称为 G 的**独立数**(indepedent number),记作 $\alpha(G)$. G 中最大团的基数,称为 G 的**团数**(clique number),有时记作 $c(G)$. G 中最大匹配的基数,称为 G 的**边独立数**(edge-independence number),记作 $\alpha'(G)$.

定义 10.9.3 设 $G=(V,E)$,$C\subseteq V$,C 包含 E 的每条边的至少一个端点,则称 C 为 G 的**点覆盖**(vertex cover). 设 $L\subseteq E$,若 G 的每一点都是 L 中某边的端点,则称 L 是 G 的**边覆盖**(edge covering). G 中最小覆盖的基数,称为 G 的**覆盖数**(covering number),记作 $\beta(G)$;

G 中最小边覆盖的基数称为 G 的**边覆盖数**(edge covering number),记作 $\beta'(G)$.

定理 10.9.4 设 $G=(V,E)$为简单图,$|V|=n$,$|E|=m$,则 G 的独立数 $\alpha(G)$有以下估计式:

(1) $\alpha(G)\geqslant\frac{n^2}{2m+n}$,

等式成立当且仅当 G 的每一连通分支是阶数相同的团.

(2) $\alpha(G)\geqslant\frac{2n-m}{3}$,

等式成立当且仅当 G 的每一连通分支是 2-团或 3-团.

定理 10.9.5 设 $G=(V,E)$是一个图,则有独立数与覆盖数之间的关系:

(1) $S\subseteq V$,则 S 是独立集$\Leftrightarrow V\backslash S$ 的点覆盖.

(2) $\alpha(G)+\beta(G)=|V(G)|$.

(3) 对非空图 G 有 $\alpha'(G)+\beta'(G)=|V(G)|$.

(4) 对二分图 G 且 $\delta>0$ 有

$$\alpha(G)=\beta'(G),\quad \alpha'(G)=\beta(G).$$

不含$(m+1)$-团或不含$(m+1)$-独立集的图的边数的估值见 10.3 节.

定理 10.9.6 含有 k-团或 l-独立集的图(Ramsey 定理的图论形式).

Ramsey 定理 对任何正整数 k 和 l,都存在一个最小的正整数 $\gamma(k,l)$,对任何阶数 $n\geqslant\gamma(k,l)$ 的简单图,或者包含 k-团,或者包含 l-独立集. 数 $\gamma(k,l)$ 称为 Ramsey 数. 已知的 Ramsey 数 $\gamma(k,l)$ 见表 8.6.

广义 Ramsey 定理 设 $k_1,k_2\cdots,k_m$ 为 m 个正整数,用 m 种颜色对完全图 K_n 的边着色,则存在最小的正整数 $\gamma(k_1,k_2,\cdots,k_m)$ 使 K_n 的着色必含有第一种颜色的 k_1-团,或第 2 种颜色的 k_2-团,……,或第 m 种颜色的 k_m-团.

10.10 一些特殊图类

定义 10.10.1 Petersen 图:该图最初是由 Petersen 用来作为一个没有割边的 3-正则图不能分解为 3 个 1-因子的和的一个例子. 后来,它陆续被发现具有许多特殊的性质,在很多问题中都被作为一个特例或反例,以致可以说,Petersen 图是图论中最重要的一个特殊的图(图 10.1). 它的性质有

(1) 3-正则;且是一个 5-笼;

(2) 非平面图;

(3) 第二型边色数图;

(4) 非哈密尔顿图;但有哈密尔顿路,且满足条件:$\omega(G-S)\leqslant|S|,\forall S\subseteq V(G)$(参看 11.4 节);

(5) 是点传递图但不是 Cayley 图.

定义 10.10.2 广义 Petersen 图类 $P(n,2)$:设 n 为 $\geqslant5$ 的奇数,由 n 个外点组成一个外圈,圈内有 n 个内点,每个内点与对应的外点相连,相隔的两内点相连. 具有性质:是第一型边色数图.

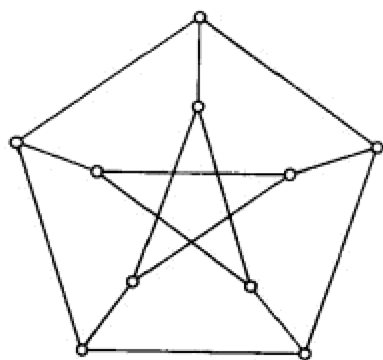


图 10.1

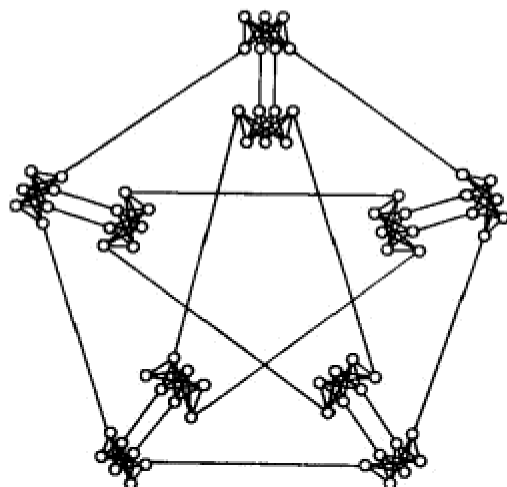


图 10.2

定义 10.10.3 Meredith 图类 $M_{k,m}$：该类图是在 Petersen 图的基础上构造出来的. 在 Petersen 图中将每一个点用 $K_{k,k-1}$ 代替,并连成一个 k-正则图(图 10.2). 它具有以下性质:

设$|V|=n,m=\lfloor \frac{n}{3} \rfloor$,则当 $m=$偶数时,G 是第一型边色数图,否则是第二型的.

定义 10.10.4 设 $r(k,l)$为 Ramsey 数(见 8.17 节),则顶点数为 $r(k,l)-1$,既不包含 k-团也不包含 l-独立集的图称为 **Ramsey(k,l)图**. 见图 10.3～图 10.6.

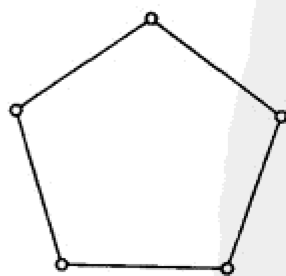


图 10.3 Ramsey(3,3)图

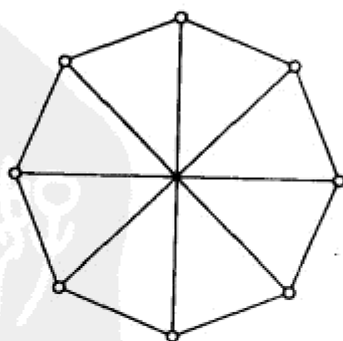


图 10.4 Ramsey(3,4)图

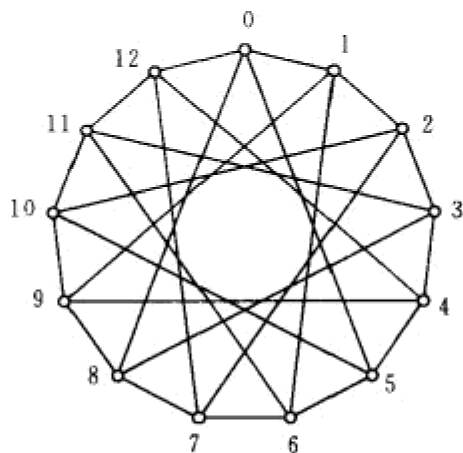


图 10.5 Ramsey(3,5)图

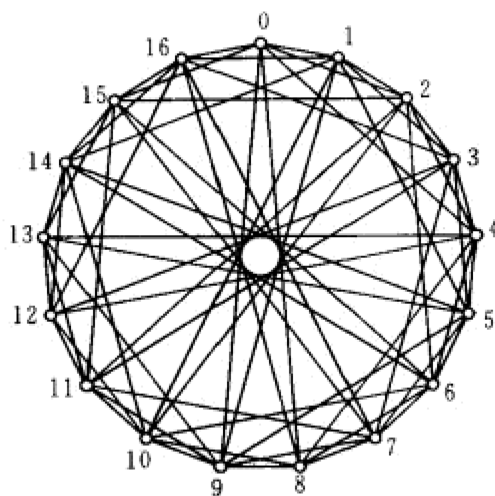


图 10.6 Ramsey(4,4)图

定义 10.10.5 设 G 是一个直径为 d 的 k 次正则图，$n=|v(G)|$. 如果

$$n = 1+k+k(k-1)+\cdots+k(k-1)^{d-1},$$

则称 G 为一个 **Moore 图**.

定理 10.10.6 直径为 d、次数为 k、围长为 g 的连通图为 Moore 图的充要条件是 $g=2d+1$.

定理 10.10.7 设 G 是直径为 d 的 k 次 Moore 图，则当 $k=2$ 时，G 为多边形，且 $(2d+1)$-边形也一定是一个 Moore 图. 当 $k\geqslant 3$ 时，必有 $d=2$ 且 $k\in\{3,7,57\}$.

定义 10.10.8 设 Γ 是一个有限群，Ω 为 Γ 的一个子集且满足 $1\notin\Omega$，$\forall x\in\Omega$ 有 $x^{-1}\in\Omega$. 群 Γ 关于子集 Ω 的 **Cayley 图** G 定义如下：

$$V(G)=\Gamma, E(G)=\{(g,h)\mid g^{-1}h\in\Omega\},$$

记作 $G=G(\Gamma,\Omega)$.

定理 10.10.9 Cayley 图的性质

(1) $G(\Gamma,\Omega)$连通的充要条件是$\langle\Omega\rangle=G$.

(2) Cayley 图是顶点传递图.

(3) Γ的左正则表示$L(\Gamma)\leqslant \mathrm{Aut}(G)$.

例 10.10.10 设$\Gamma=S_3$,$\Omega=\{(12),(23),(13)\}$,则 Cayley 图 $G=G(S_3,\Omega)$同构于$K_{3,3}$,如图 10.7 所示.

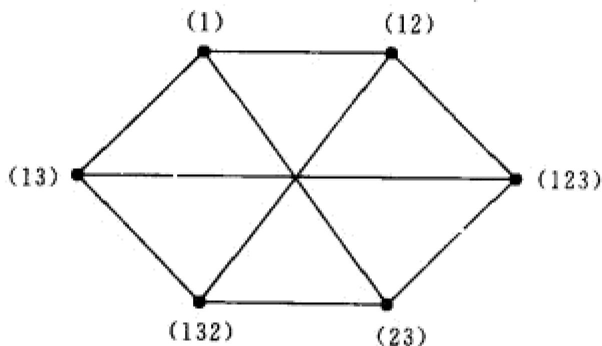


图 10.7

并非每个点传递图都是 Cayley 图,Petersen 图是点传递图,但它不是 Cayley 图.

定义 10.10.11 **循环图**(circulant graph):设图 G 的邻接矩阵$\boldsymbol{A}(G)$为以下形式的循环矩阵:

$$\boldsymbol{A}(G)=\begin{bmatrix} 0 & a_2 & a_3 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & 0 & a_2 & \cdots & a_{n-3} & a_{n-2} \\ a_{n-2} & a_{n-1} & 0 & \cdots & a_{n-4} & a_{n-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_3 & a_4 & a_5 & \cdots & 0 & a_2 \\ a_2 & a_3 & a_4 & \cdots & a_{n-1} & 0 \end{bmatrix}$$

循环图有以下性质:

(1) 循环图是正则图;

(2) 循环图的特征值为

$$\lambda_i = \sum_{j=1}^{n} a_j \omega^{(j-1)i}, i = 0,1,\cdots,n-1,$$

其中 $a_1=0,\omega=e^{\frac{2\pi}{n}i}$为 n 次单位根.

循环图亦可直接定义如下：设 $G_n(r_1,r_2,\cdots,r_k)$为 n 阶图，$0<r_1<r_2<\cdots<r_k$，$V=\{v_1,v_2,\cdots,v_n\}$，$E=\{(v_i,v_{i\pm r_j})\mid i=1,2,\cdots,n,j=1,2,\cdots,k\}$，其中 $i\pm r_j$ 为模 n 的运算.

循环图也可以简单地定义为循环群上的 Cayley 图.

定义 10.10.12 设图 $G=(V,E)$，$|V|=n$，$|E|=m$，若存在单射 θ: $V\to[0,m]$(称 θ 为 V 上的标号)满足：$\forall e_1,e_2\in E$ 且 $e_1\neq e_2$ 有 $\theta'(e_1)\neq\theta'(e_2)$，其中 $\theta'(e)=|\theta(u)-\theta(v)|$，$e=uv$. 即任意两条边的标号差都不相同，则称 G 为**优美图**(graceful graph)，称 θ 为 G 的一个优美标号.

猜想 10.10.13 **优美树猜想**(graceful tree conjecture, A. Rosa, 1966)：所有的树都是优美的.

(参看马克杰，《优美图》，北京大学出版社，1991.)

定义 10.10.14 设 G 是一个简单图，如果 G 的每个导出子图的色数 χ 等于其极大团的点数 ω，则称 G 为**完美图**(perfect graph).

设 G 是一个二分图，则 G 的补图、线图及线图的补图都是完美图.

定理 10.10.15 完美图定理 完美图的补图是完美图.

猜想 10.10.16 强完美图猜想 图 G 为完美图当且仅当 G 和 $\overline{G}$ 都不含奇圈这样的导出子图.

定义 10.10.17 若图 G 不是完美的，但它的所有真导出子图都是完美的，则称 G 为**临界非完美图**. 利用临界概念，可以把强完美图猜想如下：奇圈及其补图是仅有的临界非完美图.

定义 10.10.18 围长为 g，点数最少的 k-正则图称为一个 (k,g)-**笼**(cage). 并有以下结果：

(1) 设 $f(k,g)$为(k,g)-笼的点数,则 $f(2,g)=g$,对 $k\geqslant 3$, 有

$$f(k,g)=\begin{cases}\dfrac{k(k-1)^{\gamma}-2}{k-2}, g=2\gamma+1;\\[2ex] \dfrac{2(k-1)^{\gamma}-2}{k-2}, g=2\gamma.\end{cases}$$

(2) $(2,g)$-笼为 g-圈;$(k,3)$-笼为 K_{k+1},$(k,4)$-笼为 $K_{k,k}$.

(3) 对 $k\geqslant 3$ 和 $g\geqslant 5$,上述(1)中等式成立仅当 $g=5$ 和 $k=3$, 7,57 或 $g=6,8,12$.

(4) 对于 $g\geqslant 3$,存在一个$(3,g)$-笼,对于 $g=3$ 到 8,存在唯一的$(3,g)$-笼.

已知的$(3,g)$-笼列于表 10.1.

表 10.1　已知的$(3,g)$-笼

g	$(3,g)$-笼	g	$(3,g)$-笼
3	K_4	6	Heawood 图
4	$K_{3,3}$	7	McGee 图
5	Petersen 图	8	Tutte-Coxeter 图

图 10.8 为 Heawood 图/(3,6)-笼.

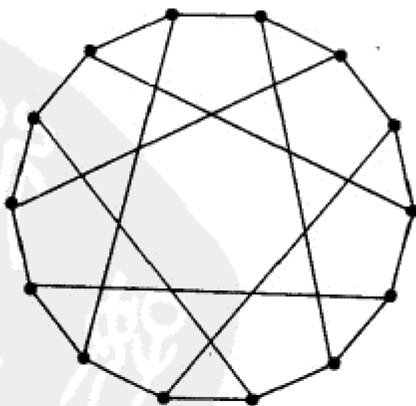


图　10.8

图 10.9 为 McGee 图/(3,7)-笼：图 10.9 按所注的标号的并.

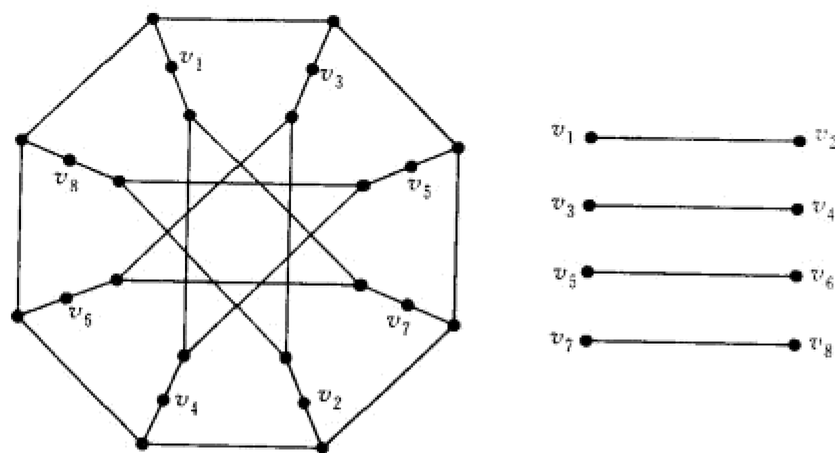


图 10.9

图 10.10 为 Tutte-Coxeter 图(3,8)-笼：所示两图按标号的并.

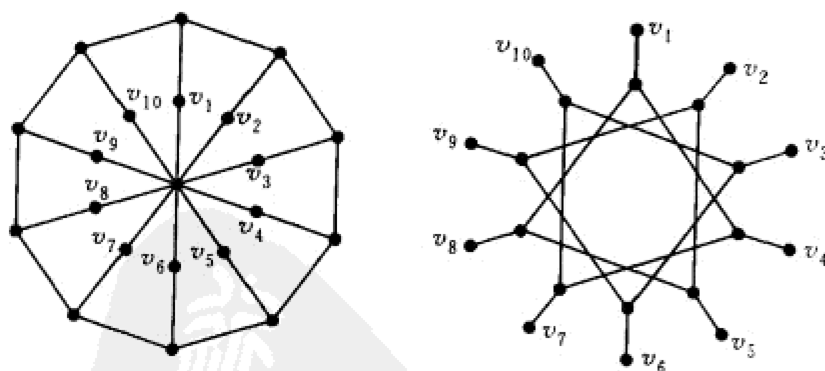


图 10.10

定义 10.10.19 *k*-立方图(*k*-cube)：有 2^k 个点，每个点对应一个 k 位二进制数，两点相邻的充分必要条件是它们对应的二进制数恰有一位不同.

图 10.11 为 3-立方图.

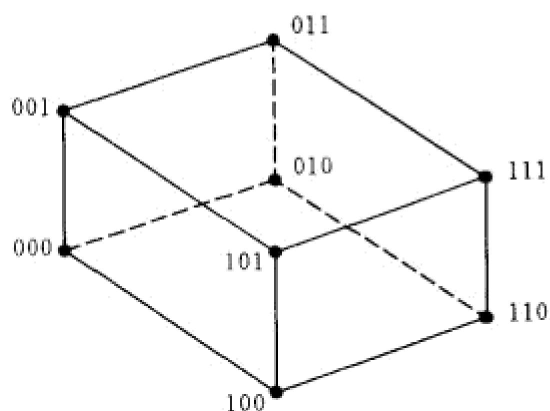


图 10.11

图 10.12 为 4-立方图.

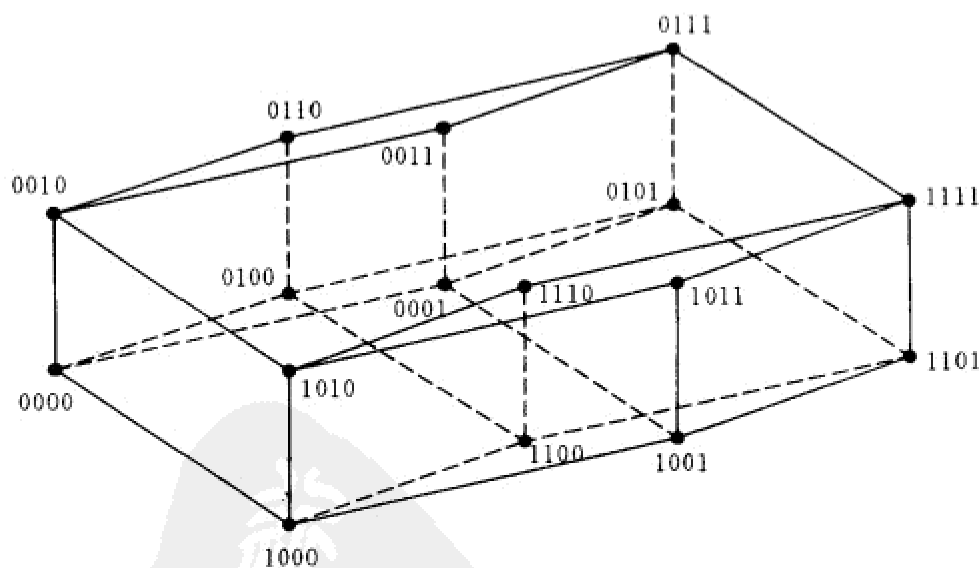


图 10.12

定义 10.10.20 度序列最优的非哈密尔顿图 $C_{m,n}$：设 $n \geqslant 2m$，令

$$C_{m,n} = K_m \vee (K_m^c + K_{n-2m}),$$

则 $C_{m,n}$有以下性质：

(1) 若 G 是一个 $|V(G)| \geqslant 3$ 的非哈密尔顿简单图，则有某个

$C_{m,n}$ 其度序列优于 G 的度序列(所谓度序列的优劣指：设两个图的度序是分别为 $S_1=(d_1,d_2,\cdots,d_n)$，$S_2=(d_1',d_2',\cdots,d_n')$，若有 $d_i\geqslant d_i'(i=1,2,\cdots,n)$，则称度序列 S_1 优于度序列 S_2).

(2) $C_{m,n}$的度序列为

$$(\underbrace{m,\cdots,m}_{m个},\underbrace{n-m-1,\cdots,n-m-1}_{n-2m个},\underbrace{n-1,\cdots,n-1}_{m个}).$$

(3) $C_{m,n}$的边数

$$|E(C_{m,n})|=\frac{1}{2}[m^2+(n-2m)(n-m-1)+m(n-1)].$$

图 10.13 为图 $C_{m,n}$. 图 10.14 为图 $C_{1,5}$. 图 10.15 为图 $C_{2,5}$.



图 10.13

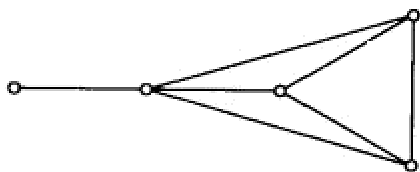


图 10.14

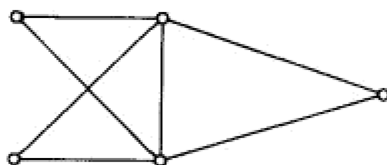


图 10.15

定义 10.10.21 不含($m+1$)-团的边数最多的图 $T_{m,n}$(Turan 图)：设 $T_{m,n}$为 n 阶不含($m+1$)-团的边数最多的图. 它的构造如下：$T_{m,n}$是一个完全 m 分图，每一部分有$\left\lceil\frac{n}{m}\right\rceil$个或$\left\lfloor\frac{n}{m}\right\rfloor$个点，即同一部分的点互相不相邻，不同部分的点之间均有边相连，参看(定理 10.3.7). 设 $n=mt+r,0\leqslant r<m$，则

$$T_{m,n}=K_{\underbrace{t,\cdots,t}_{m-r个},\underbrace{t+1,\cdots,t+1}_{r个}},$$

图 10.16 为图 $T_{3,8}$.

定义 10.10.22 连通度为 m 的边数最少的图 $H_{m,n}$：设 $H_{m,n}$

是连通度为 m 的 n 阶图，则 $H_{m,n}$ 的构造如下：

(1) 当 $m=2\gamma$ 时，设 $V(H_{m,n})=\{0,1,2,3,\cdots,n-1\}$，则 $E(H_{m,n})$ 为 $i-\gamma\leqslant j+\gamma\pmod{n}$ 时有 $ij\in E$.

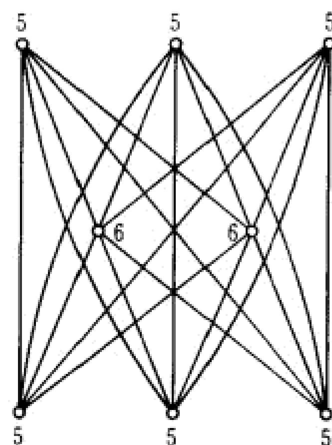


图 10.16

(2) 当 $m=2\gamma+1$ 且 n 为偶数时，先按(1)作出 $H_{2\gamma,n}$，然后再连接 i 到 $i+\frac{n}{2}\left(0\leqslant i<\frac{n}{2}\right)$.

(3) 当 $m=2\gamma+1$ 且 n 为奇数时，先按(1)作出 $H_{2\gamma,n}$，然后再连接 0 到 $\frac{n-1}{2}$ 和 $\frac{n+1}{2}$，i 到 $i+\frac{n+1}{2}\left(1\leqslant i<\frac{n-1}{2}\right)$.

且有

$$|E(H_{m,n})|=\left\lceil\frac{mn}{2}\right\rceil.$$

图 10.17 为图 $H_{4,8}$，图 10.18 为图 $H_{5,8}$，图 10.19 为图 $H_{5,9}$.

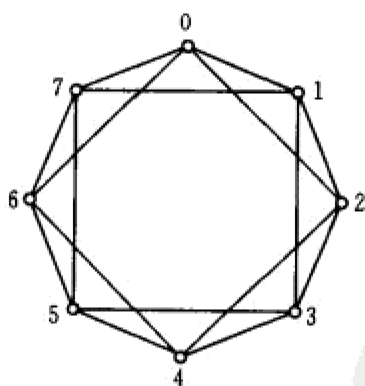


图 10.17

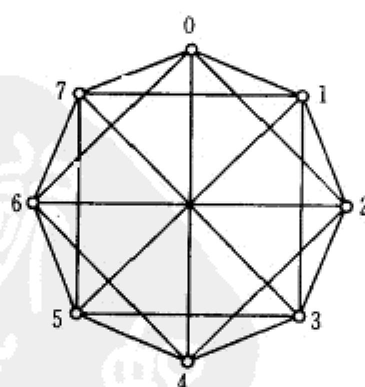


图 10.18

定义 10.10.23 有人曾猜想，每一个 3-正则的 3-连通可平面图含有一个哈密尔顿圈. Tutte 作出了一个 46 阶的 3-正则 3-连通的可平面图，但不是哈密尔顿的，从而否定了此猜想. 这个图常被称为 **Tutte 图**(图 10.20).

图 10.21 为 Herschel 图，该图的特点是二分图，非哈密尔顿图，但有哈密尔顿路.

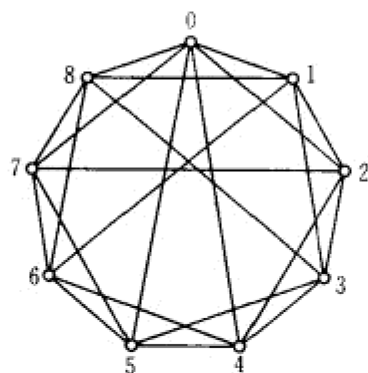
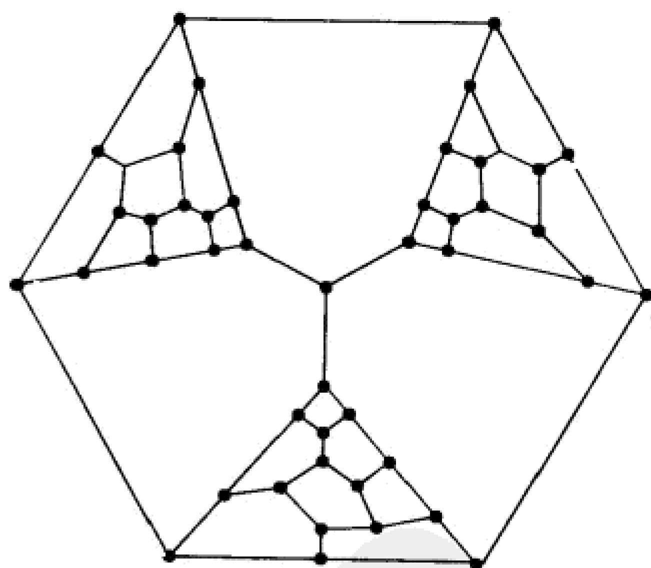


图 10.19


图 10.20

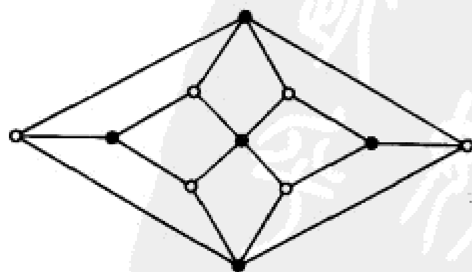

图 10.21

图 10.22 为 Grotzsch 图，是围长为 4 的点着色 4-临界图.

图 10.23 为 Coxeter 图，此图具有以下性质：

(1) 第二型边色图.

(2) 顶点传递的，含哈密尔顿路但不含哈密尔顿圈.

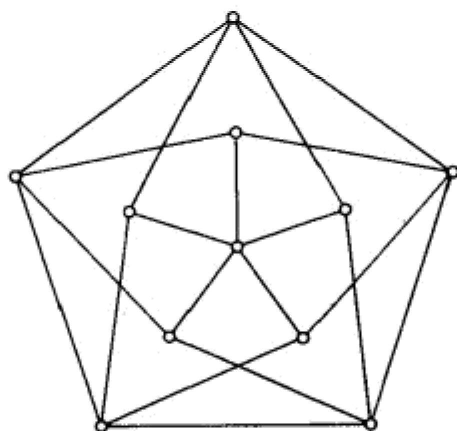


图 10.22

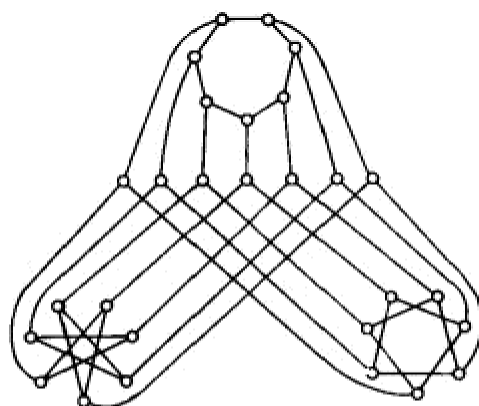


图 10.23

定义 10.10.24 Mobius 梯 M_s：有 $2s$ 个点. 在圈 C_{2s} 上连接对顶点的边所构成的 3-正则图. 具有以下性质：

(1) M_s 的特征值为

$$\lambda_i = 2\cos\pi j/s + (-1)^i j,\quad j = 0,1,\cdots,2s-1.$$

(2) M_s 的色多项式为

$$P_s(u) = (u^2-3u+3)^s + (u-1)[(3-u)^s-(1-u)^s]-1.$$

定义 10.10.25 超八面体图(hyperoctahendron) H_s，即为 $K_{2,2,\cdots,2}$，$2s$ 个点的 s 分图，具有以下性质：

(1) 其特征值谱为

$$\mathrm{Spec}H_s = \begin{pmatrix} 2s-2 & 0 & -2 \\ 1 & s & s-1 \end{pmatrix}.$$

(2) 其色多项式有以下递推公式：

$P_1(u) = u^2$，

$P_s(u) = u(u-1)P_{s-1}(u-2) + uP_{s-1}(u-1), s \geqslant 2.$

11 图论中若干问题

11.1 图的连通性

11.1.1 基本概念

定义 11.1.1 若图中任何两点之间都有路连接，则称此图是**连通图**(connected).

定义 11.1.2 图 G 中的一个最大连通子图称为 G 中的一个**连通分支**(component)；G 的连通分支的个数称为 G 的**连通分支数**，记作 $\omega(G)$.

定义 11.1.3 设 G 为连通图，$v\in V(G)$，若 $G-v$ 不连通，则称 v 为**割点**(cut vertex). $e\in E(G)$，若 $G-e$ 不连通，则称 e 为 G 的一个**割边**(cut edge)，割边又称**桥**(bridge).

定义 11.1.4 设 $G=(V,E)$，$V'\subset V$，若 $G-V'$ 不连通，则称 V' 是 G 的**点割集**(vertex cut). $E'\subset E$，若 $G-E'$ 不连通，则称 E' 是 G 的一个**边割集**(edge cut).

定义 11.1.5 G 中最小割集的基数称为 G 的**连通度**(connectivity)，记作 $\kappa(G)$. G 中最小边割集的基数，称为**边连通度**(edge connectivity)，记作 $\kappa'(G)$.

定义 11.1.6 若 $\kappa(G)\geqslant k$，则称 G 是一个 k-**连通图**(k-connected graph). 若 $\kappa'(G)\geqslant k$，则称 G 是一个 k-**边连通图**(k-edge-connected graph).

定义 11.1.7 图内的一个极大 2-连通子图称为图中的一个**块**(block). 一个 2-连通图可称为一个块.

定义 11.1.8 若 G 是 k-连通的，且 $\forall e \in E(G)$，$E-e$ 不再是 k-连通的，即 $\kappa(G-e)<k$，则称 G 是极小 k-**连通图**(minimally k-connected graph).

11.1.2 连通图的性质

定理 11.1.9 Menger 定理　设 G 是简单图，则 G 是 k-连通的充分必要条件是 G 中任何两点之间有 k 条独立路(指无公共点的路).

定理 11.1.10 设 G 是连通图，则 G 是树的充分必要条件是 G 的每一条边是割边.

定理 11.1.11 若图 G 是连通的，则 $|E(G)| \geqslant |V(G)|-1$.

定理 11.1.12 若 $G=(V,E)$ 不是 k-连通的，则存在 V_1, V_2: $V_1 \cap V_2 = \varnothing$, $|V_1| = n_1 \geqslant 1$, $|V_2| = n_2 \geqslant 1$, $n_1+n_2+k-1=n$ 使

$$\forall v_i \in V_i (i=1,2) \qquad 有\ d(v_i) \leqslant n_i + k - 2.$$

定理 11.1.13 设图 G 的度序列为 $d(v_1) \leqslant d(v_2) \leqslant \cdots \leqslant d(v_n)$，若存在 $k(0 \leqslant k \leqslant n)$ 使 $d(v_i) \leqslant j+k-1$, $j=1,2,\cdots,n-1-d(v_{n-k+1})$，则 G 是 k-连通的.

定理 11.1.14 设 G 为 n 阶图，则有：

(1) $2\delta+2-n \leqslant \kappa(G) \leqslant \delta$.

(2) $\forall v \in V(G), e \in E(G)$ 有

$$\kappa(G)-1 \leqslant \kappa(G-v) \leqslant \kappa(G)$$
$$\kappa'(G)-1 \leqslant \kappa'(G-v) \leqslant \kappa'(G)$$

(3) 设 S 是点数为 n，边数为 m 的图的集合，则有

$$\max_S \kappa(G) = \max_S \kappa'(G) = \left\lfloor \frac{2m}{n} \right\rfloor.$$

定理 11.1.15 3-连通图构造定理(Tutte 定理)　G 是 3-连通图的充分必要条件是 G 是一个轮或对一个轮重复施以下列两

种运算所得到的图：

(1) 加一条边；

(2) 分裂任何一个次数$\geqslant 4$的点x：用两个相邻的点x',x''代替x,将x的每一个邻点与x'或x''相连,并使x'与x''的次数都大于或等于3.

定理 11.1.16 极小2-连通图的性质

(1) 设G是2-连通图,则G是极小的充分必要条件是G中任何一个圈中没有弦(即两端在圈上的边).

(2) n阶极小2-连通图至少含有$(n+4)/3$个2次点,且对$n\equiv -1,0(\mathrm{mod}\ 3)$这是最少的可能.

(3) 设G是n阶极小2-连通图且$n\geqslant 4$,则$|E(G)|\leqslant 2n-4$,且$K_{2,n-2}$是唯一的一个n阶,边数为$2n-4$的极小2-连通图.

定理 11.1.17 极小k-连通图的性质 设$G=(V,E)$是极小k-连通图,则有：

(1) k次点的个数$\geqslant \dfrac{(k-1)n+2}{2k-1}$.

(2) 当$n\geqslant 3k-2$时,$|E(G)|\leqslant k(n-k)$. 当$n\geqslant 3k-1$时有$|E(G)|=k(n-k)$的充分必要条件是$G\cong K_{k,n-k}$.

11.2 图的平面性

11.2.1 平面图及有关参数

定义 11.2.1 一个图G若能画在一个平面上而使它的边仅在顶点处相交,则称G为一个平面图(planar graph),否则称为非平面图.(有些书上称G为可平面化的或可平面图,而把已画在平面上其边仅在顶点处相交的图称为平面图.)

定义 11.2.2 平面图将平面分为一些连通闭域,每个闭域称为一个面(face),无界的面称为**外面**(outer face),其余的面称为内

面(inner face). 某个面 f 的边界所含的边数，称为 f 的**次**(degree)记作 $d(f)$. 设 $G(V,E,F)$ 为平面图，其中 F 是 G 的面的集合，则有下面定理.

定理 11.2.3

(1) 欧拉多面体公式(Euler polyhedron formula) $|V|-|E|+|F|=2$.

(2) $|E|\leqslant 3|V|-6, |V|\geqslant 3$.

(3) 若 G 是 2-连通的，且不含三角形，则 $|E|\leqslant 2|V|-4$.

(4) 若 G 中每一个面是三角形，则 $|E|\leqslant 2|V|-6$.

(5) 若 G 中每一个面是 4-圈，则 $|E|=2|V|-4$.

(6) 若 G 中每一个面是 k-圈，则 $|E|=k(|V|-2)/(k-2)$.

(7) 对 $|V|\geqslant 4$, G 中至少有 4 个点次数不超过 5.

(8) $\sum\limits_{f\in F} d(f)=2|E|$.

11.2.2 平面图的条件及性质

定理 11.2.4 K_5, $K_{3,3}$ 是非平面图.

定理 11.2.5 Kuratowski 定理 一个图是平面图的充分必要条件是它不含 K_5 或 $K_{3,3}$ 的细分作为它的子图(图的细分见定义 10.7.10).

定理 11.2.6 Harary 定理 一个图是平面图的充分必要条件是它没有可以收缩到 K_5 或 $K_{3,3}$ 的子图(图的收缩见定义 10.7.8).

定义 11.2.7 设 $G=(V,E,F)$ 是一个平面图，若对它不能再加入边而保持其平面性，则称 G 是**极大平面图**(maximal planar graph).

极大平面图有以下性质.

定理 11.2.8 (1) 若 G 是极大平面图，则每个面是一个三角

形,且$|E|=3|V|-6$.

(2) 若G是阶数$\geqslant 4$的极大平面图,则G是3-连通的.

定义 11.2.9 设$G(V,E,F)$是一个平面图,令$G^*=(V^*,E^*,F^*)$,其中$V^*=F$,E^*定义如下:$e^*=(f_1,f_2)\in E^*\Leftrightarrow e$在面$f_1$与面$f_2$的公共边界上. 则称$G^*$为$G$的**对偶图**(dual graph). 对偶图有以下性质.

定理 11.2.10 (1) 平面图G的对偶图G^*仍为平面图.

(2) 若G是连通的平面图,则$G^{**}=G$.

(3) 同构的平面图可能有非同构的对偶图. 这是由于一个图可能有不同的平面化方法.

例 11.2.11 $G_1=G_2$,但它们有不同构的对偶图,见图 11.1.

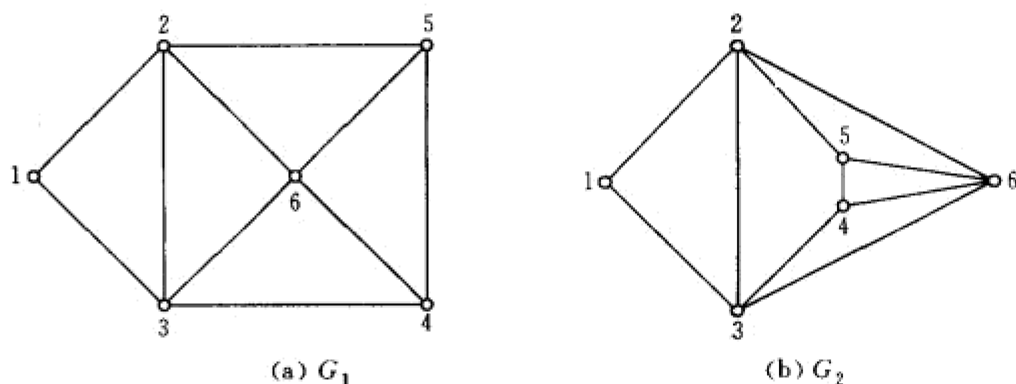


图 11.1

定理 11.2.12 平面图的连通性有以下结果:

(1) 4-连通平面图是 Hamilton 的.

(2) 每一个5-连通平面图至少有12个点.

(3) 并非每个极大平面图是 Hamilton 的.

(4) 无6-连通的平面图.

(5) 若G是一个极大平面图且每个三角形界定一个区域,则G是 Hamilton 的.

定义 11.2.13 若一个平面图可使它的所有点位于同一个面的边界上，通常将此面画成外面，这样的图称为**外平面图**(outerplanar graph). 如果一个外平面图不能再加边而保持它的外平面性，则称它为**极大外平面图**(maximal outerplanar graph).

定理 11.2.14 外平面图有以下性质：

(1) 设 G 是连通的，且不是一条路，则 G 是外平面图的充分必要条件是 G 不含 K_4 或 $K_{2,3}$ 的细分作为子图.

(2) 一个 2-连通的 n 阶外平面图是一个 n-圈上加一些不相交的弦.

定理 11.2.15 极大外平面图的性质：

(1) 一个 n 阶极大外平面图是一个 n 边形的一个三角形剖分.

(2) 一个 n 阶极大外平面图有 $n-2$ 个内面，$2n-3$ 条边.

(3) 至少有 2 个二次点，至少有 3 个点次数 $\leqslant 3$.

(4) 连通度 $\kappa(G)=2$.

11.3 图的拓扑不变量

11.3.1 定向曲面与非定向曲面

定义 11.3.1 定向曲面(orientable surface)：球面 S_0，环面(torus)S_1，双环面 S_2，三环面 S_3，…(见图 11.2).



图 11.2

构成：在球面上加 k 个环柄(handle)构成 S_k. 任何一个图可以画在一个定向曲面上使没有相交边.

定义 11.3.2 Möbius 带是一个既非闭的又非定向的曲面，其边界为一连续闭曲线（见图 11.3）. 一般地非定向曲面(nonorientable surface)是指：曲面上一个法向量沿曲面上某一连续闭曲线运动不离开曲面也不越过曲面的边界回到原来的点而该法向量反向.

将球面上开一个洞，接上一个 Möbius 带形成一个闭曲面称为**射影平面**(projective plane). 接上的 Möbius 带称为一个**交叉套**(crosscap). 接上 k 个交叉套的曲面记为 N_k, $k=1,2,\cdots$. 任何一个图可以画在某个 N_k 上面使得没有相交边.

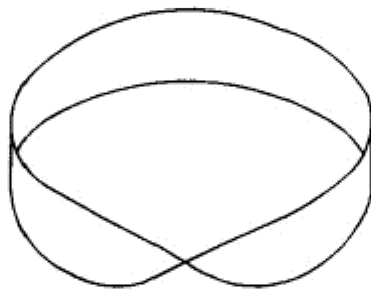


图 11.3

定理 11.3.3 根据曲面分类定理，任何一个定向曲面都可以由球面上加上若干个环柄得到. 任何一个非定向曲面都可以由球面上接上若干个交叉套得到.

定义 11.3.4 由球面添加了 k 个环柄的定向曲面 S_k 的**亏格**(genus)就定义为这个非负整数 k，记为 $\gamma(S_k)=k$. 而由球面添加了 k 个交叉套所得到的曲面 N_k 的(**非定向**)**亏格**((nonorientable) genus)定义为这个正整数 k，记为 $\tilde{\gamma}(N_k)=k$.

定义 11.3.5 曲面 S 的欧拉特征 $\chi(S)$(Euler characteristic)定义为：

$$\chi(S_h)=2-2h, \text{对定向曲面 } S_h.$$

$$\chi(N_k)=2-k, \text{对非定向曲面 } N_k.$$

11.3.2 图的曲面嵌入与亏格

定义 11.3.6 所谓把一个图 G **嵌入**(embedding)到一个曲面 S 上，是指把 G 的顶点和边都画在 S 上，使任何两条边至多只在

顶点处相交. 如果图 G 被嵌入到了曲面 S 上,则 $S-G$ 是一些开集的并,其中那些拓扑同胚于一个开圆盘或 2-胞腔(2-cells)的开集叫这个嵌入的**面**(faces),如果所有的开集都是面,则称该嵌入为 2-胞腔嵌入(2-cell embedding).

定义 11.3.7 图 G 的亏格定义为它可以嵌入到其上的定向曲面的最小亏格,一般记为 $\gamma(G)$. 亏格为 $\gamma(G)$ 的嵌入叫图 G 的极小嵌入(minimal embedding). 连通图的极小嵌入一定是 2-胞腔嵌入.

一个图的非定向亏格,指它可以嵌入的非定向曲面的最小亏格.

定理 11.3.8 如果连通图 G 在曲面 S 上有一个极小嵌入,则有

$$p-q+f=\chi(S),$$

其中 $p=|V(G)|$,$q=|E(G)|$,而 f 是嵌入的面数,具体地,有

$$\begin{cases} p-q+f=2-2h, \text{其中 } h \text{ 是图 } G \text{ 的亏格.} \\ p-q+f=2-k, \text{其中 } k \text{ 是图 } G \text{ 的非定向亏格.} \end{cases}$$

称它们为推广的欧拉多面体公式.

定理 11.3.9 $G=(V,E)$ 是连通的,$|V|=p\geqslant 3$,$|E|=g$,$\gamma=\gamma(G)$ 为图的亏格,则有

(1) $\gamma\geqslant\frac{1}{6}q-\frac{1}{2}(p-2)$.

(2) 若 G 内无三角形,则

$$\gamma\geqslant\frac{1}{4}q-\frac{1}{2}(p-2).$$

(3) 若每个面是三角形,则

$$q=3(p-2+2\gamma).$$

(4) 若每个面是四边形,则

$$g=2(p-2+2\gamma).$$

定理 11.3.10 若干种图的亏格

(1) p 阶完全图的亏格为

$$\gamma(K_p)=\left\lceil \frac{(p-3)(p-4)}{12} \right\rceil.$$

(2) 完全二分图的亏格为

$$\gamma(K_{m,n})=\left\lceil \frac{(m-2)(n-2)}{4} \right\rceil.$$

(3) k-立方图 Q_k 的亏格为

$$\gamma(Q_k)=1+(k-4)2^{k-3}.$$

定义 11.3.11 将图 G 分解为平面图的并的最小数目,称为 G 的**厚度**(thickness),记作 $\theta(G)$.

定理 11.3.12 (1) 完全图的厚度

$$\theta(K_p)\geqslant\left\lfloor \frac{p-7}{6} \right\rfloor.$$

$$p=5-8,\quad \theta(K_p)=2,$$

$$\theta(K_9)=\theta(K_{10})=\theta(K_{16})=3,$$

$p\neq 4 \pmod 6$ 且 $p\neq 9$ 时,或 $p\geqslant 46$,$\theta(K_p)=\left\lfloor \frac{p+7}{6} \right\rfloor$,

$\theta(K_{22})=4$,$\theta(K_{28})=5$,$\theta(K_{34})=6$,$\theta(K_{40})=7$.

(2) 完全二分图的厚度

$$\theta(K_{m,n})=\left\lceil \frac{mn}{2(m+n-2)} \right\rceil.$$

(3) 立方图 Q_n 的厚度

$$\theta(Q_n)=\left\lceil \frac{n+1}{4} \right\rceil.$$

定义 11.3.13 图的**叉数**(crossing numbers)定义为把它画在平面上时两交边对的最小数目,记为 $\nu(G)$. 显然 $\nu(G)=0$ 当且仅当 G 是可平面图.

定理 11.3.14 (1) $\nu(K_p)\leqslant\frac{1}{4}\left[\frac{p}{2}\right]\left[\frac{p-1}{2}\right]\left[\frac{p-2}{2}\right]\left[\frac{p-3}{2}\right]$.

(2) $\nu(K_{m,n})\leqslant\left[\frac{m}{2}\right]\left[\frac{m-1}{2}\right]\left[\frac{n}{2}\right]\left[\frac{n-1}{2}\right]$.

(3) $\nu(C_3\times C_n)=n$,当 $n\geqslant 3$.

(4) $\nu(C_4\times C_n)=2n$,当 $n\geqslant 4$.

(5) $\nu(K_4\times C_n)=3n$,当 $n\geqslant 3$.

11.4 图的 Hamilton 问题

11.4.1 Hamilton 图的必要条件

定理 11.4.1 Hamilton 图的必要条件 若 $G=(V,E)$是 Hamilton 图,则对 V 中任何非空子集 S 有 $\omega(G-S)\leqslant|S|$,这里 $\omega(H)$表示图 H 的连通分支数.

11.4.2 Hamilton 图的充分条件

定理 11.4.2 最小次条件或 Dirac 条件(Dirac condition) $n(n\geqslant 3)$阶简单图 G 若满足 $\delta\geqslant n/2$,则 G 是 Hamilton 图.

定理 11.4.3 次数条件 设 G 是简单图,$|V(G)|=n\geqslant 3$,若对任何 $k\left(1\leqslant k<\frac{n-1}{2}\right)$,次数$\leqslant k$ 的点数少于 k;当 n 是奇数时,还需满足次数$\leqslant(n-1)/2$ 的点数目$\leqslant(n-1)/2$,则 G 是 Hamilton 图.

定理 11.4.4 次数和条件或 Ore 条件 设 $G=(V,E)$为 n 阶简单图,若 $\forall u,v\in V$ 且 $uv\notin E$ 有 $d(u)+d(v)\geqslant n$,则 G 是 Hamilton 图.

定理 11.4.5 次序列条件或 Chvatal 条件 设 n 阶简单图 G 的次序列为 $d_1\leqslant d_2\leqslant\cdots\leqslant d_n$,若对每一个 $k\left(d_k\leqslant k<\frac{n}{2}\right)$有 $d_{n-k}\geqslant n-k$,则 G 是 Hamilton 图.

定理 11.4.6 边数条件 设 $G=(V,E)$是简单图,$|V|=n\geqslant 3$,$|E|=m$,若有 $m>\binom{n-1}{2}+1$,则 G 是 Hamilton 图. 且当

$m=\binom{n-1}{2}+1$ 时，非 Hamilton 图只有 $C_{1,n}$ 和 $C_{2,5}$. 这里 $C_{m,n}$ 的意义为 $C_{m,n}=K_m \vee (K_m^c+K_{n-2m})$.

定理 11.4.7 范更华条件 设 G 是简单 2-连通图，$|V(G)|=n\geqslant 3$，如果 $d(v,u)=2 \Rightarrow \max(d(v),d(u))\geqslant n/2$，则 G 是 Hamilton 图.

11.4.3 Hamilton 图的几个等价条件

定理 11.4.8 设 $G=(V,E)$ 是 n 阶简单图，若有 $u,v\in V$，且 $uv\notin E$ 满足 $d(u)+d(v)\geqslant n$，则 G 是 Hamilton 图的充分必要条件是 $G+uv$ 是 Hamilton 图.

定理 11.4.9 设 G 是 n 阶简单图，则 G 是 Hamilton 图的充分必要条件是 G 的闭包 $C(G)$ 是 Hamilton 图.

其中 C 的闭包 $C(G)$ 的定义如下. 逐次进行以下运算：当 $uv\notin E$ 且 $d(u)+d(v)\geqslant n$ 时，则在 G 中增加边 uv，直至不能再加入边为止，所得的图就是 $C(G)$.

11.4.4 图的泛圈性

定理 11.4.10 Hakimi 和 Schmeichel 定理 n 阶简单图 G 的非降次序列 $d_1\leqslant d_2\leqslant\cdots\leqslant d_n$ 满足条件：

$$d_k\leqslant k<\frac{1}{2}n\Rightarrow d_{n-k}\geqslant n-k,$$

则 G 是**泛圈图**(pancycle graph)或为二分图. 泛圈图指图内存在长度为 $3,\cdots,n$ 的圈.

定理 11.4.11 Bondy 定理 $n(n\geqslant 3)$ 阶简单图 G 满足条件：$\forall x,y\in V(G)$ 且 $xy\notin E(G)$ 有

$$d(x)+d(y)\geqslant n,$$

则 G 是泛圈图或 $K_{\frac{n}{2},\frac{n}{2}}$.

11.5 图的匹配与因子分解问题

11.5.1 基本概念

定义 11.5.1 设 $G=(V,E)$ 是一个图，一个边独立集 $M\subseteq E$ 称为 G 的一个**匹配**. G 的非空生成子图称为 G 的**因子**(factor). 若 G 可分解为一些边不相交的因子的并，就称为 G 的**因子分解**(factorization)，并称 G 是这些因子的和.

定义 11.5.2 若 G 的一个因子是 k-正则的，则称它是 G 的一个 **k-因子**. 若 G 有 k-因子分解，则称 G 是**可 k-因子化的**(factorable).

定义 11.5.3 设 M 是 G 的一个匹配，$v\in V(G)$，若 v 是 M 中某一条边的端点，则称 **M 饱和 v；或 v 是 M-饱和的**.

定义 11.5.4 设 M 是 G 中的一个匹配，M 饱和 G 中的每一点，则称 M 是**完全匹配**(perfect matching). 若不存在 M'，使 $|M'|>|M|$，则称 M 是 G 中的最大匹配(maximum matching).

定义 11.5.5 设 M 是 G 的一个匹配，P 是 G 中一条路，若 P 上的边交替地在 M 中和 $E\backslash M$ 中，则称 P 是一条 **M-交替路**. 设 P 是 G 中一条 M-交替路，其起点与终点均不是 M-饱和的，则称 P 是一条 **M-可增路**(augmenting path).

11.5.2 图中存在完全匹配的条件

定理 11.5.6 (1) 设 $G=(V,E)$，则 G 中有完全匹配的充分必要条件是，对任何非空子集 $S\subseteq V$，有 $\omega_1(G-S)\leqslant|S|$，其中 $\omega_1(H)$ 是图 H 中含有奇数个点的分支数目.

(2) 每一个无割边的 3-正则图有完全匹配.

(3) 每一个 k-正则的二分图($k>0$)G 有完全匹配.

(4) 设 $G=(X,Y,E)$ 是一个二分图，则 G 有饱和 X 的每一点

的匹配的充分必要条件是对任何非空子集 $S \subseteq X$ 均有 $|N(S)| \geqslant |S|$，其中 $N(S)$ 是 S 的邻集.

定理 11.5.7 设 M 是 G 的一个匹配，则 M 是 G 的最大匹配的充分必要条件是 G 中不包含 M-可增路.

11.5.3 匹配与覆盖的关系

定理 11.5.8 (1) 对 G 中的任何匹配 M 与任何覆盖 K 有 $|M| \leqslant |K|$.

(2) 若匹配 M 与覆盖 K 满足 $|M| = |K|$，则 M 是最大匹配，K 是最小覆盖.

(3) 设 $G=(X,Y,E)$ 是二分图，M 是匹配，K 是覆盖，则 M 是最大匹配，K 是最小覆盖 $\Leftrightarrow |M| = |K|$.

定理 11.5.9 已知的可 k-因子化的图：

(1) K_{2n} 可 1-因子化.

(2) 每一个正则二分图可 1-因子化.

(3) K_{2n+1} 是 n 个生成圈之和.

(4) K_{2n} 是一个 1-因子和 $n-1$ 个生成圈之和.

(5) 设 G 是连通图，则 G 可 2-因子化的充分必要条件是 G 是 $2k$-正则的.

(6) 每一个没有割边的三次正则图是一个 1-因子和 2-因子之和.

(7) 一个连通图可 2-因子化的充要条件是它是偶正则图.

定义 11.5.10 一个非空图可分解为一些生成林的和，且每一个生成林至少包含一条边. 图 G 分解为这样的生成林的最少数目称为这个图的**荫度**(arboricity)，记作 $\gamma(G)$.

定理 11.5.11 设 G 是一个 (p,q) 图，q_k 是 G 中任何一个 k-子图中最大边数，则荫度为

$$\gamma(G) = \max_k \left[\frac{q_k}{k-1}\right].$$

完全图与完全二分图的亏度

$$\gamma(K_p)=\left[\frac{p}{2}\right],$$

$$\gamma(K_{m,n})=\left[\frac{mn}{m+n-1}\right].$$

11.6 图的着色问题

11.6.1 点着色与边着色

定义 11.6.1 设 $G=(V,E)$ 是图，$A=\{a_1,a_2,\cdots,a_k\}$ 是 k 种颜色的集合，则每一个映射 $f: V\to A$ 称为 G 的一个**着色**(coloring)或 k-着色，每一个映射 $g: E\to A$ 称为 G 的一个**边着色**(edge coloring)或 k-边着色.

定义 11.6.2 设 f 是图 G 的一个着色或边着色，若相邻元素着不同的颜色，则称 f 是一个**正常着色**(proper coloring). 一般情况下，不加说明的图的着色指正常着色.

定义 11.6.3 图 G 的正常 k-着色的最小 k 值，称为 G 的**色数**(chromatic number)，记作 $\chi(G)$；图 G 的正常 k-边着色的最小 k 值，称为 G 的**边色数**(edge chromatic number)，记作 $\chi'(G)$.

定义 11.6.4 若 G 有一个 k-正常着色，则称 G 是 **k-色图**(k-chromatic graph). 若 $\chi(G)=k$，$\forall v\in V(G)$ 有 $\chi(G-V)<k$，则称 G 是 **k-色临界图**(k-critical graph).

k-色临界图有以下性质.

定理 11.6.5 (1) 若 G 是一个 k-色临界图，则 $\delta(G)\geqslant k-1$.

(2) 若 G 是一个 k-色临界图，$k\geqslant 3$，则 G 是哈密尔顿图，或 G 的周长 $\geqslant 2k-2$.

定义 11.6.6 若图 G 有一个 k-边正常着色，则称 G 是一个 **k-边色图**(k-edge-chromatic graph)；若 $\chi'(G)=k$，$\forall e\in E(G)$ 有 $\chi'(G-e)<k$，则称 G 为 **k-边色临界图**(k-edge-critical graph).

k-色临界图有以下性质.

定理 11.6.7 (1) 设$G=(V,E)$,Δ为最大次,若G是Δ-边色临界的,则$\forall uv\in E$有

$$d(u)+d(v)\geqslant \Delta+2.$$

(2) 边色临界图无割点.

(3) 若G是第二类边色图,则对每一个满足$2\leqslant k\leqslant \Delta(G)$的$k$,$G$包含一个$k$-边色临界图.

定义 11.6.8 设$\chi(G)=k$,若G的任一k-着色所对应的$V(G)$的划分都相同,则称G是**唯一k-着色图**(uniquely k coloriable graph).

唯一着色图有以下性质.

定理 11.6.9 (1) 在一个唯一k-色图的k-着色中,由任何两个色组的并导出的子图是连通的.

(2) 每一个唯一k-色图是$(k-1)$-连通的.

(3) 对所有$k\geqslant 3$有一个唯一k-色图,它不包含同构于K_k的子图.

例 11.6.10 图 11.4 是一个唯一 3-着色图.

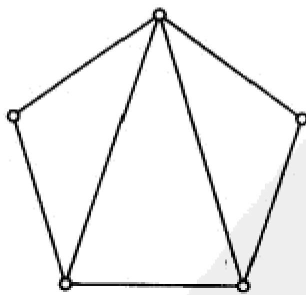


图 11.4

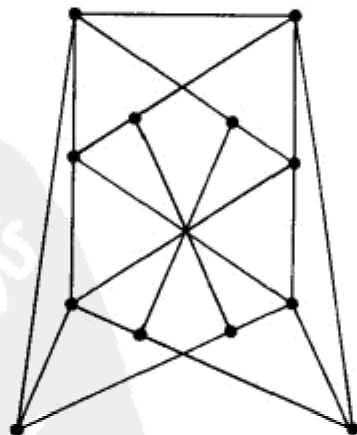


图 11.5

例 11.6.11 图 11.5 是一个没有 K_3 的唯一 3-着色图.

11.6.2 色数 $\chi(G)$ 的性质

定理 11.6.12 设 $G=(V,E)$，则有：

(1) $\chi(G)\leqslant\Delta(G)+1$.

(2) 若 G 是简单图且非奇圈也非完全图，则

$$\chi(G)\leqslant\Delta(G).$$

(3) Hajos 猜想(1961) 若 G 是 k-色图，则 G 包含 K_k 的一个细分.（该猜想对 $k=4$ 已证明. 已有人证明对 $k\geqslant 7$ 此猜想不成立.）

(4) 若 G 是一个 (n,m) 简单图，则

$$\chi(G)\geqslant\frac{n^2}{n^2-2m}.$$

(5) 设 $uv\notin E(G)$，记 $(u\cdot v)G$ 为将 u 与 v 等同起来所得之图，则

$$\chi(G)\leqslant\chi((u\cdot v)G)\leqslant 1+\chi(G).$$

(6) 设 G 是 n 阶图，$1<k\leqslant n$，G 不是 K_k 和空图 S_{n-k} 的不相交并，则有

$$m\leqslant\binom{k}{2}\Rightarrow\chi(G)<k.$$

(7) 设 G 是 n 阶图，$\alpha(G)$ 为 G 的独立数，则 $n/\alpha(G)\leqslant\chi(G)\leqslant n-\alpha(G)+1$.

11.6.3 边色数 $\chi'(G)$ 的性质

定理 11.6.13 Vizing 定理 设 G 是无环的 p-重图，则

$$\Delta\leqslant\chi'(G)\leqslant\Delta+p,\chi'(G)\leqslant\lfloor 3\Delta/2\rfloor,$$

且存在 $\chi'(G)=\Delta+p$ 的图.

定理 11.6.14 若 G 是简单图，则

$$\chi'(G) = \Delta \text{ 或 } \chi'(G) = \Delta + 1,$$

称满足 $\chi'(G)=\Delta$ 的图为**第一类边色图**(first class for edge coloring),称满足 $\chi'(G)=\Delta+1$ 的图为**第二类边色图**(second class for edge coloring).

第一类边色图有:K_{2n},二分图,广义 Petersen 图,m 为偶数的 Meredith 图 $M_{n,m}$(见定义 10.10.3),rt=偶数的 $K_{\underbrace{r,\cdots,r}_{t个}}$.

第二类边色图有:K_{2n+1},Petersen 图,奇数阶正则图,$m>\left[\frac{n}{2}\right]\cdot\Delta$ 的简单(n,m)图,m 为奇数的 Meredith 图 $M_{n,m}$,Coxeter 图,rt=奇数的 $K_{r,\cdots,r}$.

定理 11.6.15 某些图为边色数:

(1) $\chi'(K_n)=\begin{cases} n-1, & n=\text{偶数}; \\ n, & n=\text{奇数}. \end{cases}$

(2) 设 G 是二分图,则 $\chi'(G)=\Delta(G)$.

(3) $\chi'(K_{\underbrace{r,\cdots,r}_{t个}})=\begin{cases} r(t-1)+1, & rt=\text{奇数}; \\ r(t-1), & rt=\text{偶数}. \end{cases}$

11.6.4 平面图的着色

定理 11.6.16 **四色定理(猜想)**每个平面图是 4-可着色的.

定理 11.6.17 与四色猜想等价的命题:

(1) 每个平面图是 4-可面着色的.

(2) 每个 2-边连通的 3-正则平面图是 3-可着色的.

定理 11.6.18 五色定理 每个平面图是 5-可着色的.

定理 11.6.19 关于第一类边色数图有以下结果:

(1) $\Delta\geqslant 8$ 的平面图是第一类边色数图.

(2) 猜想:$\Delta\geqslant 6$ 的平面图是第一类边色数图.

(3) 设 G 是外平面图,则 G 是第一类边色数图的充分必要条

件是 G 不是奇圈.

定义 11.6.20 用 λ 种颜色对图 G 的顶点着色，不同的着色方法数是 λ 的多项式，称为 G 的着色多项式(chromatic polynomial)记作 $P_G(\lambda)$或 $P_\lambda(G)$. $P_G(\lambda)$有以下性质.

定理 11.6.21 (1) 递推公式 设 $G=(V,E)$为简单图，$e\in E$，则有

$$P_G(\lambda) = P_{G-e}(\lambda) - P_{G\cdot e}(\lambda),$$

$uv \notin E$，则有

$$P_G(\lambda) = P_{G+uv}(\lambda) + P_{(u\cdot v)G}(\lambda).$$

(2) $\deg P_G(\lambda)=n=|V|$.

(3) $P_G(\lambda)$的系数有以下性质：

1) $P_G(\lambda)$的首项系数为 1，常数项为 0；

2) $P_G(\lambda)$的系数为正负交替的整数；

3) $P_G(\lambda)$的系数的绝对值随 λ 的次数呈单峰形；

4) $P_G(\lambda)$的不为 0 的系数的最小次数等于 G 的连通分支数；

5) λ^{n-1} 的系数为 $-|E|$.

11.6.5 图的运算的色多项式

定理 11.6.22 (1) 当 $G_1\cap G_2=\varnothing$时，有

$$P_\lambda(G_1 \cup G_2) = P_\lambda(G_1)P_\lambda(G_2).$$

(2) 当 $G_1\cap G_2=K_q$ 时，有

$$P_\lambda(G_1 \cup G_2) = \frac{P_\lambda(G_1)\cdot P_\lambda(G_2)}{[\lambda]_q},$$

其中 $[\lambda]_q=\lambda(\lambda-1)\cdots(\lambda-q+1)$.

(3) 当 G_1 与 G_2 为两个图，$G_1\vee G_2$ 表示两个图的连接，即将 G_1 的每一点与 G_2 的每个点用边相连.

$$P_\lambda(G_1 \vee G_2) = P_\lambda(G_1)\circ P_\lambda(G_2),$$

其中多项式之间的运算$\circ$定义如下：首先将每个色多项式写成如下形式

$$P_\lambda(G_1) = \sum m_r[\lambda]_\gamma,$$

其中 m_r 为 $V(G_1)$的 γ-色剖分数,$[\lambda]_\gamma=\lambda(\lambda-1)\cdots(\lambda-\gamma+1)$.

$P_\lambda(G_2) = \sum m'_s [\lambda]_s$, 意义同上. 然后按规律$[\lambda]_\gamma[\lambda]_s = [\lambda]_{\gamma+s}$ 作乘积.

例: $P_\lambda(K_{3,3})=P_\lambda(N_3)\circ P_\lambda(N_3)=([\lambda]_3+3[\lambda]_2+[\lambda]_1)^2$

$$=[\lambda]_6+6[\lambda]_5+11[\lambda]_4+6[\lambda]_3+[\lambda]_2$$

$$=\lambda^6-9\lambda^5+36\lambda^4-75\lambda^3+78\lambda^2-31\lambda.$$

定理 11.6.23 几类图的色多项式

(1) 空图的色多项式为 λ^n.

(2) 完全图的色多项式为

$$P_{K_n}(\lambda) = \lambda(\lambda-1)\cdots(\lambda-n+1).$$

(3) T 为树的充分必要条件为 T 的色多项式为 $\lambda(\lambda-1)^{n-1}$.

(4) 圈的色多项式为$(\lambda-1)^n+(-1)^n(\lambda-1)$.

(5) 轮的色多项式为

$$P_{W_{n+1}}(\lambda) = \lambda(\lambda-2)^n + (-1)^n\lambda(\lambda-2).$$

(6) 连通图 G 的色多项式 $P_G(\lambda)\leqslant\lambda(\lambda-1)^{n-1}$.

定义 11.6.24 设 $G=(V,E)$,每一个映射 $f: V\cup E\to A$ 称为 G 的一个**全着色**(total coloring). 若 f 满足相邻元素着不同的颜色,则称 f 是正常全着色. 图 G 有正常 k-全着色的最小的 k 值,称为 G 的**全色数**(total chromatic number),记作 $\chi_T(G)$.

猜想 11.6.25 全色数猜想 设 $\chi_T(G)$是图 G 的全色数,则对任何图 G 有

$$\Delta(G)+1\leqslant\chi_T(G)\leqslant\Delta(G)+2.$$

(此猜想尚未证明,只对一些特殊图类证明了它是正确的.)

定义 11.6.26 满足 $\chi_T(G)=\Delta(G)+1$ 的图称为**第一类全色数图**(first class for total coloring),满足 $\chi_T(G)=\Delta(G)+2$ 的图

称为**第二类全色数图**.

定义 11.6.27 设 $G=(V,E,F)$ 是平面图，则对 G 可定义以下几种**全着色**：

(1) 点边全着色及点边全色数 $\chi_T(G)$.

(2) 边面全着色及边面全色数 $\chi_{ef}(G)$.

(3) 点面全着色点面全色数 $\chi_{vf}(G)$.

(4) 点边面全着色点及边面全色数 $\chi_{vef}(G)$.

11.7 图的代数理论

定理 11.7.1 邻接矩阵的性质 设 $G=(V,E)$ 为一个 (n,m) 图，$\mathbf{A}=\mathbf{A}(G)$ 是 G 的邻接矩阵（参见定义 10.2.4），则 $\mathbf{A}$ 有以下性质：

(1) 设

$$\mathbf{A}^k=(a_{ij}^{(k)})_{n\times n},$$

则 $a_{ij}^{(k)}$ 为从 v_i 到 v_j 的长度为 k 的通道的数目. 从 v_i 到 v_j 的距离是使 $a_{ij}^{(k)}\neq 0$ 的最小的 k 值.

(2) $\mathbf{A}$ 的行列式可表为

$$\det\mathbf{A}=\sum_{(H)}(-1)^{r(H)}2^{s(H)},$$

其中 H 为 G 的边圈生成子图（即 H 的每一分支或为一条边或为一个圈），$\mathrm{r}(H)$ 为 H 的秩，$\mathrm{s}(H)=m-n+\omega(G)$ 为 H 的**余秩**(corank)，和式对 G 的所有边圈生成子图求和.

定理 11.7.2 关联矩阵的性质 设 $G=(V,E)$ 为一个 (n,m) 图，$\mathbf{C}=\mathbf{C}(G)$ 为 G 的关联矩阵（参见定义 10.2.5），则 $\mathbf{C}$ 有以下性质：

(1) $\mathbf{CC}^{\mathrm{T}}=\boldsymbol{\Delta}-\mathbf{A}$

其中 $\boldsymbol{\Delta}=\mathrm{diag}(d_1,d_2,\cdots,d_n)$，$d_i$ 为 v_i 的度，$\mathbf{A}=\mathbf{A}(G)$ 为 G 的邻接

矩阵.

(2) G 是连通的充分必要条件是秩$(\boldsymbol{C})=n-1$.

(3) 秩$(\boldsymbol{C})$=图 G 的秩$=n-\omega(G)$,其中 $\omega(G)$ 为 G 的连通分支数.

(4) 设 $\boldsymbol{C}_1(G)$为 $\boldsymbol{C}(G)$去掉任一行所得之矩阵,称为**次关联矩阵**,则 $\boldsymbol{C}_1(G)$的一个 $n-1$ 阶子阵为非奇异的充分必要条件是该子阵所对应的边组成 G 的一棵生成树.

定义 11.7.3 设 $G=(V,E)$为(n,m)阶连通图,则 G 的圈空间(见定义 10.5.6)中全部向量的个数为

$$s=2^{m-n+1}-1,$$

每个向量对应 G 中一个闭迹. 设这些向量为 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_s$,令

$$b_{ij}=\begin{cases}1,\text{当边 } e_j \text{ 在闭迹 } \boldsymbol{c}_i \text{ 中},\\0,\text{否则},\end{cases}$$

则矩阵 $\boldsymbol{B}=(b_{ij})_{n\times n}$ 称为 G 的**圈矩阵**(cycle matrix),且有秩$(\boldsymbol{B}(G))=m-n+1$.

定义 11.7.4 设图 $G=(V,E)$的邻接矩阵为 $\boldsymbol{A}=\boldsymbol{A}(G)$,则 $\boldsymbol{A}$ 的特征值称为 **G 的特征值**(eigenvalue of graph G),G 的全部特征值称为 G 的**谱**(spectra),通常表示为

$$\operatorname{spec} G=\begin{pmatrix}\lambda_0 & \lambda_1 & \cdots & \lambda_{s-1}\\ m(\lambda_0) & m(\lambda_1) & \cdots & m(\lambda_{s-1})\end{pmatrix},$$

其中 $\lambda_0>\lambda_1>\cdots>\lambda_{s-1}$ 为 G 的 s 个不同的特征值,$m(\lambda_i)$为 λ_i 的重数. G 的最大特征值称为 G 的**谱半径**(spectral radius).

定理 11.7.5 图 G 的特征多项式就是 G 的邻接矩阵 $\boldsymbol{A}(G)$的特征多项式,记作 $P(G;\lambda)$. 设

$$P(G;\lambda)=|\lambda\boldsymbol{I}-\boldsymbol{A}(G)|=\lambda^n+c_1\lambda^{n-1}+\cdots+c_n,$$

则有以下性质:

(1) $c_1=0$;

(2) $-c_2=|E(G)|$;

(3) $-c_3$ 为 G 中三角形的个数的 2 倍；

(4) $(-1)^i c_i = \sum_{|H|=i} (-1)^{r(H)} 2^{s(H)}, 1 \leqslant i \leqslant n$,

其中 H 为 G 中的边圈子图，r(H)是 H 的秩，s(H)是 H 的余秩(定义 11.7.1).

定理 11.7.6　谱半径与最大次(最小次)的关系

$$\delta(G) \leqslant \lambda_{\max}(G) \leqslant \Delta(G).$$

定理 11.7.7　导出子图的特征值　设 H 是 G 的点导出子图，则有

$$\lambda_{\min}(G) \leqslant \lambda_{\min}(H) \leqslant \lambda_{\max}(H) \leqslant \lambda_{\max}(G).$$

定理 11.7.8　特征值与色数的关系　设 $\chi(G)$是 G 的色数，则有

$$1 + \frac{\lambda_{\max}(G)}{-\lambda_{\min}(G)} \leqslant \chi(G) \leqslant 1 + \lambda_{\max}(G).$$

表 11.1 为若干类图的谱.

定理 11.7.9　图的特征值的界

(1) 对任意(n,m)阶图 G 有

$$\lambda_1(G) \leqslant (-1 + \sqrt{1+8m})/2,$$

且等式成立当且仅当 $G=K_k$+空图.

(2) 对任意(n,m)阶图 G 有

$$-\sqrt{2m(i-1)/n(n-i+1)} \leqslant \lambda_i \leqslant \sqrt{2m(n-i)/ni},$$
$$i = 1,2,\cdots,n.$$

(3) 对任意简单图 G 有

$\lambda_n(G) \geqslant -\sqrt{(n/2)\lfloor \frac{n+1}{2} \rfloor}$，且等式成立当且仅当 $G=K_{\lfloor \frac{n}{2} \rfloor, \lfloor \frac{n+1}{2} \rfloor}$.

(4) 设 G 为边数等于$\binom{k}{2}$的图，则有 $\lambda_1(G) \leqslant k-1$，且等式成立当且仅当 $G=K_k$+空图.

(5) 对 n 阶连通图 G 有以下结果

$$2\cos\frac{\pi}{n+1}=\lambda_1(P_n)\leqslant\lambda_1(G)\leqslant\lambda_1(K_n)=n-1.$$

表 11.1 已知的若干类图的谱

图	谱
完全图 K_n	$\begin{pmatrix} n-1 & -1 \\ 1 & n-1 \end{pmatrix}$
路 P_n	$\lambda_i=2\cos\frac{2\pi i}{n+1}, i=1,2,\cdots,n$
圈 C_n n 为奇数	$\begin{pmatrix} 2 & 2\cos\frac{2\pi}{n} & \cdots & 2\cos\frac{(n-1)\pi}{n} \\ 1 & 2 & \cdots & 2 \end{pmatrix}$
圈 C_n n 为偶数	$\begin{pmatrix} 2 & 2\cos\frac{2\pi}{n} & \cdots & 2\cos\frac{(n-2)\pi}{n} & -2 \\ 1 & 2 & \cdots & 2 & 1 \end{pmatrix}$
完全二分图 $K_{a,b}$	$\begin{pmatrix} \sqrt{ab} & 0 & -\sqrt{ab} \\ 1 & a+b-2 & 1 \end{pmatrix}$
Petersen 图	$\begin{pmatrix} 3 & 1 & -2 \\ 1 & 5 & 4 \end{pmatrix}$
超八面体图 $H_s=K_{2,2,\cdots,2}$	$\begin{pmatrix} 2s-2 & 0 & -2 \\ 1 & s & s-1 \end{pmatrix}$
循环图 G $(\mathbf{A}(G))_1=(a_1a_2\cdots a_n)$	$\lambda_k=\sum_{j=1}^{n}a_j\omega^{(j-1)k}, \omega=e^{\frac{2\pi}{n}i}$, $k=0,1,2,\cdots,n-1$
Mobius 梯图 M_h	$\lambda_i=2\cos\frac{\pi i}{h}+(-1)^i, i=0,1,2,\cdots,2h-1$

(6) 对(n,m)阶连通图G有

$\lambda_1(G)\leqslant\sqrt{2m-n+1}$,且等式成立当且仅当$G=K_{1,n-1}$或$K_n$.

(7) 设G为连通的唯一圈图,则有

$$2=\lambda_1(C_n)\leqslant\lambda_1(G)\leqslant\lambda(S_n^3),$$

其中S_n^3为$K_{1,n-1}$加一连接两个一次顶点的边.

(8) 设T_n为n阶树,则有

$$2\cos\frac{\pi}{n+1}=\lambda_1(P_n)\leqslant\lambda_1(T_n)\leqslant\lambda_1(K_{1,n-1})=\sqrt{n-1}.$$

(9) 对n阶树T_n有

$$0\leqslant\lambda_i(T_n)\leqslant\sqrt{\lfloor(n-2)/i\rfloor},2\leqslant i\leqslant\lfloor\frac{n}{2}\rfloor,$$

当$n\equiv 1(\mathrm{mod}\ i)$时可达上界.

(10) 对k-正则图G有

1) $\lambda_1(G)=k$且当G连通时有$m(\lambda_1)=1$.

2) $|\lambda|\leqslant k$.

(11) 对n阶平面图G有

$$2\cos(\pi/(n+1))\leqslant\lambda_1(G)\leqslant 2\sqrt{2}+\sqrt{3n-15/2}.$$

(12) 对n阶外平面图G有

$$\lambda_1(G)\leqslant 1+\sqrt{2+\sqrt{2}}+\sqrt{n-5},n>5.$$

定义 11.7.10 一个图$G=(V,E)$的自同构群(参见定义10.8.2),$\Gamma(G)$称为**图G的群**(group of graph);$\Gamma(G)$作用于边集$E(G)$上所对应的置换群称为G的**线群**(line-group of G),记作$\Gamma_1(G)$.

例 11.7.11 $G=(V,E)$,$V=\{1,2,3,4\}$,$E=\{e_1,e_2,e_3,e_4,e_5\}$,见图11.6.

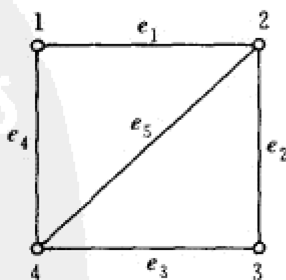


图 11.6

$\Gamma(G)=\{(1),(13),(24),(13)(24)\}$,

$\Gamma_1(G)=\{(1),(e_1e_2)(e_3e_4),(e_1e_4)(e_2e_3),(e_1e_3)(e_2e_4)\}$

一般情况下,这两个群是同构的,有以下结果.

定理 11.7.12 (1) $\Gamma(G)$与$\Gamma_1(G)$ 同构的充分必要条件是G最多有一个孤立点且K_2不是G的一个分支.

(2) 每一个图对应一个群$\Gamma(G)$;反之,任给一个有限群,也存在一个图,它的自同构群与给定的有限群同构,且这样的图有无限多.

定义 11.7.13 设$G=(V,E)$是图,它的自同构群为$\Gamma(G)$.若$\forall v_1,v_2\in V$均有$\sigma\in\Gamma(G)$使$\sigma(v_1)=v_2$,则称G是**点传递图**(vertex transitive graph);若$\forall e_1=(u_1,v_1),e_2=(u_2,v_2)\in E$均有$\sigma\in\Gamma(G)$使$\sigma(e_1)=(\sigma(u_1),\sigma(v_1))=e_2$,则称$G$是**边传递图**(edge transitive graph);若G既是点传递的,又是边传递的,则称G是**对称图**(symmetric graph).

若对所有满足$d(u,v)=d(x,y)$的u,v,x,y均有$\sigma\in\Gamma(G)$使$\sigma(u)=x,\sigma(v)=y$,则称G是**距离传递图**(distance transitive graph).

且有以下结果.

定理 11.7.14 (1) 设G是连通图,则有

G是距离可传的$\Rightarrow G$是对称的$\Rightarrow G$是顶点可传的.

(2) 每一个无孤立点的边可传图是点可传的或是二分图.

12 离散变换与反演公式

12.1 离散变换的一般形式

设有两个多项式簇：$p_k(x), q_k(x), k=0,1,2,\cdots,n$. 每个多项式 $p_k(x)$ 和 $q_k(x)$ 都是 k 次的. 若它们满足

$$\left.\begin{aligned} p_k(x) &= \sum_{i=0}^{k} \alpha_{i,k} q_i(x), \\ q_k(x) &= \sum_{i=0}^{k} \beta_{i,k} p_i(x), \\ k &= 0,1,2,\cdots,n, \end{aligned}\right\} \qquad (12.1)$$

且其中系数 $\alpha_{i,k}, \beta_{i,k}$ 满足以下的正交性：

$$\sum_{i=j}^{k} \alpha_{i,k} \beta_{j,i} = \delta_{jk} = \begin{cases} 1, & j = k, \\ 0, & j \neq k, \end{cases} \qquad (12.2)$$

则下列两式

$$\left.\begin{aligned} f(k) &= \sum_{i=0}^{k} \alpha_{i,k} g(i), \\ g(k) &= \sum_{i=0}^{k} \beta_{i,k} f(i), \\ k &= 0,1,2,\cdots,n, \end{aligned}\right\} \qquad (12.3)$$

可互相推导.

这里 $f(k), g(k)$ 是两个整标函数. 式(12.3)称为**离散变换**(discrete transform)或**反演**(inversion).

选取不同的系数 $\alpha_{i,k}, \beta_{i,k}$ 可得到不同种类的离散变换.

12.2 二项式变换

这类变换中的系数与二项式系数有关,称它们为**二项式变换**(binomial transform).

12.2.1 二项式变换的一般形式

设 $f(n),g(n),h(n),\tilde{h}(n)$ 为定义在非负整数集上的整标函数,且 $h(0)\neq 0,\tilde{h}(0)\neq 0$,则以下两式互逆:

$$\left.\begin{aligned} f(n) &= \sum_{i=0}^{n}\binom{n}{i}h(n-i)g(i), \\ g(n) &= \sum_{i=0}^{n}\binom{n}{i}\tilde{h}(n-i)f(i), \end{aligned}\right\} \tag{12.4}$$

其中 $h(i)$ 与 $\tilde{h}(i)$ 满足条件:

$$\sum_{j=0}^{i}\binom{i}{j}\tilde{h}(j)h(i-j) = \begin{cases}1, 当\ i=0, \\ 0, 当\ i>0.\end{cases} \tag{12.5}$$

选择不同的 $h(i)$ 与 $\tilde{h}(i)$ 可得不同的二项式变换.

12.2.2 常用的二项式变换

(1) 在式(12.5)中取 $h(i)=1,\tilde{h}(i)=(-1)^i$,可得以下变换:

$$\left.\begin{aligned} f(n) &= \sum_{k=0}^{n}\binom{n}{k}g(k), \\ g(n) &= \sum_{k=0}^{n}(-1)^{n+k}\binom{n}{k}f(k). \end{aligned}\right\} \tag{12.6}$$

(2) 在式(12.5)中取 $h(i)=c^i,\tilde{h}(i)=(-1)^i$,可得以下的变换:

$$
\left.\begin{aligned}
f(n) &= \sum_{k=0}^{n}\binom{n}{k}c^{n-k}g(k),\\
g(n) &= \sum_{k=0}^{n}(-1)^{n+k}\binom{n}{k}f(k).
\end{aligned}\right\} \tag{12.7}
$$

其中 c 为非零常数.

(3) 与 Stirling 数有关的二项式变换为

$$
\left.\begin{aligned}
n^{p} &= \sum_{k=0}^{n}\binom{n}{k}k!S(p,k),\\
S(n,m) &= \frac{1}{m!}\sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}k^{n},
\end{aligned}\right\} \tag{12.8}
$$

表 12.1 为若干简单的二项式变换.

表 12.1 若干简单的二项式变换

1. $a_n = \sum_{k=0}^{n}\binom{n}{k}b_k$,	$b_n = \sum_{k=0}^{n}(-1)^{k+n}\binom{n}{k}a_k$.
2. $a_n = \sum_{k=n}\binom{k}{n}b_k$,	$b_n = \sum_{k=n}(-1)^{k+n}\binom{k}{n}a_k$.
3. $a_n = \sum_{k=0}\binom{p-k}{p-n}b_k$,	$b_n = \sum_{k=0}(-1)^{k+n}\binom{p-k}{p-n}a_k$.
4. $a_n = \sum_{k=0}^{n}\binom{n+p}{k+p}b_k$,	$b_n = \sum_{k=0}^{n}(-1)^{k+n}\binom{n+p}{k+p}a_k$.
5. $a_n = \sum_{k=n}\binom{k+p}{n+p}b_k$,	$b_n = \sum_{k=n}(-1)^{k+n}\binom{k+p}{n+p}a_k$.
6. $a_n = \sum_{k=1}\frac{n!}{k!}\binom{n-1}{k-1}b_k$,	$b_n = \sum_{k=1}(-1)^{k+n}\frac{n!}{k!}\binom{n-1}{k-1}a_k$, $n=1,2,\cdots$

12.2.3 应用

(1) 用二项式变换求 S_n 中不含不动点的置换个数. 得到与问题 9.4.2 同样的结果.

设 n 次置换中无不动点的置换个数为 D_n,则其中恰有 r 个不

动点的置换个数为$\binom{n}{r}D_{n-r}$，于是有

$$\sum_{r=0}^{n}\binom{n}{r}D_{n-r} = n!$$

由二项式变换式(12.6)得到

$$D_n = \sum_{r=0}^{n}(-1)^{n+r}\binom{n}{r}r! = n!\sum_{r=0}^{n}(-1)^r\frac{1}{r!}.$$

(2) 布置问题：把 n 个若干类物体放入 m 个若干类房间的布置格式数.

设 X 为 n 个物体的集合，X 分为若干类，每一类中的物体是相同的. 定义 X 的分类方式为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 型的，指其中每类含 1 个物体的共有λ_1类，每类含 2 个物体的共有λ_2类，…，每类含 n 个物体的共有λ_n类. 显然有 $1\cdot\lambda_1+2\cdot\lambda_2+\cdots+n\cdot\lambda_n=n$. 设 A 为房间的集合，$|A|=m$，类似可定义房间的分类方式为 $1^{\mu_1}2^{\mu_2}\cdots m^{\mu_m}$ 型的. 每一个函数 $f:X\to A$ 对应一个布置，如果两个布置 f_1 与 f_2 仅仅相差同类物体的一个置换或同类房间的一个置换，则称 f_1 与 f_2 等价，每一个等价类称为一个布置格式，现确定这样的布置格式数.

设 $A(1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n},1^{\mu_1}2^{\mu_2}\cdots m^{\mu_m})$ 为全体布置格式数，$B(1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n},1^{\mu_1}2^{\mu_2}\cdots m^{\mu_m})$ 为无空房间的布置格式数. 下面来确定房间类型为 1^m 型的布置格式数.

由可重组合数可得全部布置格式数为

$$A(1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n},1^m) = \binom{m}{1}^{\lambda_1}\binom{m+1}{2}^{\lambda_2}\cdots\binom{m+n-1}{n}^{\lambda_n}. \tag{12.9}$$

设 $B(k)$ 为把 n 个物体放到 k 个两两不同类的 k 个房间的子集 K 中且无空房间的布置格式数，$A(k)$ 为允许有空房间的布置格式数，则有

$$A(m) = \sum_{k=1}^{m} \binom{m}{k} B(k),$$

由二项式变换式(12.6)可得

$$B(m) = \sum_{k=1}^{m} (-1)^{m-k} \binom{m}{k} A(k),$$

将式(12.9)代入得

$$B(1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}, 1^m) = \sum_{k=1}^{m} (-1)^{m-k} \binom{m}{k} \cdot \binom{k}{1}^{\lambda_1} \cdot \binom{k+1}{2}^{\lambda_2} \cdots \binom{k+n-1}{n}^{\lambda_n}.$$

12.3 Stirling 变换

Stirling 变换的特点是正反变换中的系数分别是第一、第二类 Stirling 函数. 设 $f(k), g(k)$ $(k=1,2,\cdots,n)$ 为两个整标函数,则以下互逆的变换

$$f(k) = \sum_{i=1}^{k} s(k,i) g(i),$$
$$g(k) = \sum_{i=1}^{k} S(k,i) f(i), \tag{12.10}$$
$$(k = 1,2,\cdots,n)$$

称为 **Stirling 变换**(Stirling transform).

其中 $s(k,i)$ 与 $S(k,i)$ 分别为第一类与第二类 Stirling 数(见 8.11 节和 8.12 节).

证明方法:由 Stirling 数的定义 $[x]_k = \sum_{i=1}^{k} s(k,i) x^i$, $x^k = \sum_{i=1}^{k} S(k,i) [x]_i$,再利用式(12.1)与(12.2)即可得到.

12.4 Möbius 变换

Möbius 变换的特点是：正变换是一简单的和式，反变换的系数是 Möbius 函数．通常称它为 Möbius 反演公式．由于许多实际问题可化为一些子问题的和，而总数容易计算，则可通过 Möbius 反演公式求得子问题的数目．Möbius 变换有广泛的应用，在组合理论中占据很重要的地位．

12.4.1 Möbius 反演公式的一般形式

定义 12.4.1 设 $\langle X,\leqslant\rangle$ 是一个局部有限（局部有限指：$\forall x,y\in X$，区间 $[x,y]$ 是一个有限集）偏序集或局部有限格．在 X 上定义函数：

$$\mu(x,y)=\begin{cases}1, & \text{当 } x=y,\\ -\sum\limits_{x\leqslant u<y}\mu(x,u), & \text{当 } x<y,\\ 0, & \text{其他}.\end{cases} \tag{12.11}$$

则称 $\mu(x,y)$ 为 $\langle X,\leqslant\rangle$ 上的 **Möbius 函数**（Möbius function）．

$f(x),g(x)$ 是 $\langle X,\leqslant\rangle$ 上的两个整数函数，则有

$$\left.\begin{aligned} f(x)&=\sum_{0\leqslant u\leqslant x}g(u),\\ g(x)&=\sum_{0\leqslant u\leqslant x}\mu(u,x)f(u),\end{aligned}\right\} \tag{12.12}$$

其中 0 元为 $\langle X,\leqslant\rangle$ 中的最小元．称(12.12)为偏序集 $\langle X,\leqslant\rangle$ 上的 **Möbius 变换**（Möbius transform）或 **Möbius 反演**（Möbius inversion）．

12.4.2 整数因子格上的 Möbius 反演公式

设 $\langle \mathbf{Z}^+,|\rangle$ 为正整数集合 $\mathbf{Z}^+$ 关于整除关系"|"的偏序集，定义

Möbius 函数如下：

$$\mu(d,n)=\begin{cases}1, & 当\ d=n,\\ (-1)^k, & 当\ d\mid n\ 且\ \dfrac{n}{d}=p_1p_2\cdots p_k,\\ 0, & 其他.\end{cases}\tag{12.13}$$

其中 $p_1,p_2,\cdots,p_k$ 为互不相同的素数.

定理 12.4.2 以下互逆式子成立：

$$\left.\begin{aligned}f(n)&=\sum_{d\mid n}g(d),\\ g(n)&=\sum_{d\mid n}\mu(d,n)f(d).\end{aligned}\right\}\tag{12.14}$$

称式(12.14)为$\langle \mathbf{Z}^+,\mid\rangle$上的 Möbius **反演公式**.

$\langle \mathbf{Z}^+,\mid\rangle$上的 Möbius 反演公式可简化如下：

$$\mu(n)=\begin{cases}1, & 当\ n=1,\\ (-1)^k, & 当\ n=p_1p_2\cdots p_k,p_1,p_2,\cdots,p_k\ 为互不相同的素数,\\ 0, & 其他.\end{cases}\tag{12.15}$$

定理 12.4.3 以下两式互逆：

$$\begin{aligned}f(n)&=\sum_{d\mid n}g(d),\\ g(n)&=\sum_{d\mid n}\mu(d)f\left(\frac{n}{d}\right)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)f(d).\end{aligned}\tag{12.16}$$

12.4.3 应用

(1) 循环字个数的确定

设 $A=\{a_1,a_2,\cdots,a_m\}$为 m 个字母的集合，$X=\{1,2,\cdots,n\}$为长度为 n 的字中的位置集合，则每一个映射 f: $X\rightarrow A$ 代表一个字：$f(1)f(2)\cdots f(n)$. 在 A^X 中定义等价关系：$f_1\sim f_2\Leftrightarrow\exists p\in$

$[0,n-1]$使$\forall i\in[1,n]$有 $f_2(i)=f_1(i+p)$，其中和式 $i+p$ 为模 n 的加法. 每一个等价类称为一个循环字. 求循环字的个数,用 $C(n,m)$表示.

下面再对循环字分类. 定义 f 的周期与本原周期如下：若有 $p\in[1,n]$使 $f(i+p)=f(i)$, $\forall i\in[1,n]$,则称 p 为 f 的周期; f 的最小周期称为本原周期,本原周期必为 n 的因子. 设 $M(p)$为本原周期为 p 的循环字的个数,每一个 p 循环字包含 p 个字,因而有

$$m^n=\sum_{p\mid n}pM(p).$$

由 Möbius 反演公式,得

$$pM(p)=\sum_{q\mid p}\mu(q,p)m^q,$$

故得循环字的总数为

$$\begin{aligned}C(n,m)&=\sum_{p\mid n}M(p)\\&=\sum_{p\mid n}\frac{1}{p}\sum_{q\mid p}\mu(q,p)m^q.\end{aligned}$$

该问题在信息论的译码问题、生物学中的遗传密码问题、声学中测定音色浓厚问题中有应用.

(2) $\mathbf{Z}_p$ 上 n 次不可约多项式的个数

设 $\mathbf{Z}_p=\{0,1,2,\cdots,p-1\}$为整数模 p(素数)的同余类域, $I_p(n)$为 $\mathbf{Z}_p$ 上 n 次不可约(首 1)多项式的个数,则有

$$p^n=\sum_{m\mid n}mI_p(m),$$

$$I_p(n)=\frac{1}{n}\sum_{m\mid n}\mu\left(\frac{n}{m}\right)p^m=\frac{1}{n}\sum_{m\mid n}\mu(m)f\left(\frac{n}{m}\right).$$

12.4.4 有限集的幂集格上的 Möbius 反演公式

设 S 为有限集,$\mathscr{P}(S)$为 S 的幂集,$(\mathscr{P}(S),\subseteq)$为 $\mathscr{P}(S)$关于包

含关系"⊆"的偏序集，在$\langle \mathscr{P}(S), \subseteq \rangle$上定义 Möbius 函数如下：$\forall A, B \in \mathscr{P}(S)$有

$$\mu(B,A) = \begin{cases} (-1)^{|A|-|B|}, & \text{当 } B \subseteq A, \\ 0, & \text{否则}. \end{cases} \tag{12.17}$$

定理 12.4.4 以下两式互逆：

$$\left.\begin{aligned} f(A) &= \sum_{H \subseteq A} g(H), \\ g(B) &= \sum_{H \subseteq B} (-1)^{|B|-|H|} f(H). \end{aligned}\right\} \tag{12.18}$$

12.4.5 有限集的划分格上的 Möbius 反演公式

设 X 为有限集，P 为 X 上的所有划分所构成的集合，在 P 中定义偏序关系"$\leqslant$"为：$P_1, P_2 \in P$，$P_1 \leqslant P_2 \Leftrightarrow$ 划分 P_1 是划分 P_2 的细分. 在$\langle P, \leqslant \rangle$上定义 Möbius 函数如下：

$$\mu(P_1, P_2) = \begin{cases} (-1)^{m+n_1+n_2+\cdots+n_m}(n_1-1)!\cdots(n_m-1)!, \\ \qquad\qquad \text{当 } P_1 \leqslant P_2 \text{ 且满足条件 } D, \\ 0, \qquad\quad \text{否则}. \end{cases} \tag{12.19}$$

其中条件 D 为：设 $P_2 = \{A_1, A_2, \cdots, A_m\}$，每一个 A_i 对应 P_1 中 n_i 个子集的并.

定理 12.4.5 以下两式互逆：

$$\left.\begin{aligned} f(P_k) &= \sum_{Q \leqslant P_k} g(Q), \\ g(P_k) &= \sum_{Q \leqslant P_k} \mu(Q, P_k) f(Q). \end{aligned}\right\} \tag{12.20}$$

例 12.4.6 设 $X = \{a, b, c\}$，$P_1 = \{X\}$，$P_2 = \{\{a, b\}, \{c\}\}$，$P_3 = \{\{a\}, \{b, c\}\}$，$P_4 = \{\{a, c\}, \{b\}\}$，$P_5 = \{\{a\}, \{b\}, \{c\}\}$，$P = \{P_1, P_2, P_3, P_4, P_5\}$，$\langle P, \leqslant \rangle$上的 Möbius 函数的值为：

$$\mu(P_k, P_k) = 1,\ k = 1, 2, 3, 4, 5.$$

$$\mu(P_2,P_1)=\mu(P_3,P_1)=\mu(P_4,P_1)=-1,$$
$$\mu(P_5,P_2)=\mu(P_5,P_3)=\mu(P_5,P_4)=-1,$$
$$\mu(P_5,P_1)=2,$$
其他情况 $\mu(P_k,P_l)=0$.

12.4.6 应用

有标号连通图的数目的确定

设 $V=\{v_1,v_2,\cdots,v_n\}$，$G=(V,E)$是任意图(可以不连通)，$\pi(G)$为由 G 决定的 V 的划分：$\pi(G)$的每一部分对应 G 的一个连通分支. 反之，设 π 为 V 的任一个划分，$C(\pi)$为具有划分 π 的所有图的个数，$D(\pi)$为具有性质 $\pi(G)\leqslant\pi$ 的图 G 的个数(这里$\leqslant$为 V 的划分格中的偏序关系). 若 π 是 $1^{k_1}2^{k_2}\cdots n^{k_n}$ 型划分，则有

$$D(\pi)=2^{\sum\limits_{i=2}^{n}k_i\binom{i}{2}}=\sum_{\sigma\leqslant\pi}C(\sigma),$$

(π 的每一部分 $V_i(j)$，$|V_i(j)|=i$，$j=1,2,\cdots,k_i$，对应的图的个数为

$$d_{ij}=2^{\binom{i}{2}},$$

故
$$D(\pi)=\prod_{i=1}^{n}\prod_{j=1}^{k_i}2^{\binom{i}{2}}=2^{\sum\limits_{i=2}^{n}k_i\binom{i}{2}}\Bigg)$$

令划分 $\pi_0=\{V\}$，则连通的有标号图的个数为 $C(\pi_0)$，由 Möbius 反演公式得

$$\begin{aligned}C(\pi_0)&=\sum_{\pi\leqslant\pi_0}\mu(\pi,\pi_0)D(\pi)\\&=\sum_{(k_1,k_2,\cdots,k_n)}(-1)^{1+\sum\limits_{i=1}^{n}k_i}\Big(\sum_{i=1}^{n}k_i-1\Big)!\\&\quad\cdot 2^{\sum\limits_{i=2}^{n}k_i\binom{i}{2}}\cdot\frac{n!}{(1!)^{k_1}(2!)^{k_2}\cdots(n!)^{k_n}K_1!K_2!\cdots K_n!}.\end{aligned}$$

其中和式取遍下列方程的所有非负整数解：

$$1 \cdot k_1 + 2 \cdot k_2 + \cdots + n \cdot k_n = n.$$

12.5 离散 Fourier 变换

Fourier 变换是将周期函数表示为 Fourier 级数，其系数是一积分式. 用离散 Fourier 变换可简化系数的计算，并适合用计算机来计算.

定义 12.5.1 设 $x(k)$，$X(k)$，$k=0,1,2,\cdots,n-1$ 分别为实数与复数序列，则以下两式互逆：

$$\left.\begin{aligned} x(k) &= \sum_{j=0}^{n-1} X(j) e^{\frac{2k\pi j}{n} i} \\ X(k) &= \frac{1}{n} \sum_{j=0}^{n-1} x(j) e^{-\frac{2k\pi j}{n} i} \end{aligned}\right\} \tag{12.21}$$

其中 $i=\sqrt{-1}$，式(12.21)称为**离散 Fourier 变换**(discrete Fourier transform).

例 12.5.2 用离散 Fourier 变换计算 Fourier 级数　设 $f(x)$ 为周期 l 的实函数，则 $f(x)$ 可表为

$$\left.\begin{aligned} f(x) &= \sum_{j=-\infty}^{\infty} C_j e^{\frac{2\pi j x}{l} i} \\ C_k &= \frac{1}{l} \int_0^l f(t) e^{-\frac{2k\pi t}{l} i} dt \\ k &= 0, \pm 1, \pm 2, \cdots \end{aligned}\right\} \tag{12.22}$$

将区间$[0,l]$分为 n 等分，令 $x_k=\frac{lk}{n}$，$k=0,1,2,\cdots,n-1$，则有

$$C_k \approx \frac{1}{n} \sum_{j=0}^{n-1} f(t_j) e^{-\frac{2\pi k j}{l} i}.$$

令

$$x(k) = f(x_k)$$

则由式(12.21)可求得 $X(k)$，有专门设计的快速算法计算 $X(k)$.

从而求得 Fourier 系数：

$$C_k = X(k), C_{-k} = \overline{X(k)}, \quad k = 0,1,2,\cdots,n-1.$$

12.6 Lagrange 变换(反演公式)

Lagrange 反演公式在有根树的计数问题中很有用. 首先我们引进一个记号,设函数 $f(t)$ 的指数型形式幂级数为 $f(t) = \sum_{n=0}^{\infty} \frac{a_n}{n!} t^n$ ，记 $C_{t^n}\{f(t)\} = a_n$.

定义 12.6.1 设 $\varphi(u)$ 是一个已知的函数,并满足 $\varphi(0)=1$. 方程 $u=t\varphi(u)$ 的解确定了 u 是 t 的函数：$u=u(t)$. $f(u)$ 是另一个给定的函数,则它的幂级数系数满足以下等式：

$$C_{t^n}\{f(u(t))\} = \frac{1}{n} C_{u^{n-1}}\{f'(u)\varphi(u)^n\},$$

此公式称为 **Lagrange 变换(反演公式)**.

例 12.6.2 我们用 Lagrange 反演公式来证明 n 阶树的数目为 n^{n-2}.

设 n 阶有根树的生成函数为 $D(x) = \sum_{n=0}^{\infty} \frac{t_n}{n!} x^n$ ，其中 t_n 为 n 阶有根树的数目. 则 $D(x)$ 满足方程 $D(x) = x\mathrm{e}^{D(x)}$ (我们暂且承认它),在 Lagrange 反演公式中取 u 为 $D(x)$, $\varphi(u)=\mathrm{e}^u$, $f(u)=u$, 则得

$$C_{x^n}\{D(x)\} = \frac{1}{n} C_{u^{n-1}}\{1 \cdot \mathrm{e}^{nu}\},$$

由于 $\mathrm{e}^{nu} = 1 + \frac{nu}{1!} + \cdots + \frac{n^n u^n}{n!} + \cdots$,得

$$\frac{t_n}{n!} = \frac{1}{n} \cdot \frac{n^{n-1}}{(n-1)!},$$

所以

$$t_n = n^{n-1}.$$

由于每个树的每个点都可作为根，所以每个树对应了 n 个有根树，故全部 n 阶树的个数为 n^{n-2}.

12.7 Lah 变换（反演公式）

定义 12.7.1 以下的互逆的变换

$$f(n) = \sum_{k=0}^{n} L_{n,k} g(k),$$

$$g(n) = \sum_{k=0}^{n} L_{n,k} f(k),$$

称为 **Lah 变换（反演公式）**，其中 $L_{n,k} = (-1)^n \frac{n!}{k!}\binom{n-1}{k-1}$ 为 Lah 数（参看 8.18 节）.

13 组合设计

13.1 区组设计与拉丁方

13.1.1 基本概念

定义 13.1.1 设 S 为有限集,称为基集. $B_1,B_2,\cdots,B_n$ 为 S 的有序或无序的子集,则子集簇 $\mathscr{B}=\{B_1,B_2,\cdots,B_n\}$ 称为 S 上的**区组设计**(block design). 每个子集 B_i 称为一个**区组**(block),允许有相同的区组. 对子集 B_i 作不同的规定,就得到各种类型的区组设计.

定义 13.1.2 若 S 的一个区组设计中每个区组是 S 的元素的全排列,则称此区组设计为**完全区组设计**,否则称为**不完全区组设计**.

定义 13.1.3 设基集为 $S=\{1,2,\cdots,n\}$,用 S 中的元素排成 $n\times n$ 的方阵,每个元素在每行与每列中恰出现一次,则此方阵称为 S 上的 n 阶**拉丁方**(Latin square). 如果把拉丁方中每一行看作一个区组,则拉丁方是有 n 个区组的完全区组设计.

定义 13.1.4 设基集为 $S=\{1,2,\cdots,n\}$,用 S 中的元素排成 $r\times n$ 的阵列,使每个元素在每行每列中无重复出现,则称此阵列为 $r\times n$ 的**拉丁矩形**(Latin rectangle). 如果把 $r\times n$ 的拉丁矩形的每一行看成一个区组,则它是具有 r 个区组的完全区组设计.

13.1.2 拉丁方与拉丁矩形的计数问题

第 1 行元素为 $1,2,\cdots,n$ 的拉丁方或拉丁矩形称为正规的拉

丁方或正规的拉丁矩形. 它们的个数记作 $LR(r,n)$，当 $r<n$ 时，$LR(r,n)$为正规的拉丁矩形的个数；$LR(n,n)$为正规拉丁方的个数. 则有以下结果.

定理 13.1.5 （1）$2\times n$ 正规拉丁矩形的个数为：

$$LR(2,n)=D(n),$$

其中 $D(n)$为没有不动点的 n 次置换的个数（见问题 9.4.2）.

（2）第 1 行为 $1,2,\cdots,n$，第 2 行为 $n,1,2,\cdots,n-1$ 的 $3\times n$ 的拉丁矩形的个数为 $T(n)$，其中 $T(n)$为夫妇问题的入座数（见例 9.2.11）.

（3）$3\times n$ 的拉丁矩形的个数为

$$LR(3,n)=\sum_{k=0}^{\left[\frac{n}{2}\right]}\binom{n}{k}D(n-k)D(k)T(n-2k),$$

其中 $D(n)$与 $T(n)$见（问题 9.4.2）与（例 9.2.11）.

（4）$LR(r,n)$的一般公式尚无，仅有以下的下界与渐近公式：

$$LR(r,n)\geqslant(n-1)!(n-2)!\cdots(n-r+1)!$$

当 $r<\sqrt[3]{n}$时有

$$LR(r,n)\approx(n!)^{r}e^{-\binom{r}{2}}.$$

（5）记 ln 为第 1 行与第 1 列均为 $1,2,\cdots,n$ 的拉丁方数目，则有 $ln\geqslant(n-2)!\ (n-3)!\ \cdots1!$

但此下界不好，见下表 13.1.

表 13.1

n	3	4	5	6	7
ln	1	4	56	9408	16942080
$(n-2)!\ (n-3)!\ \cdots1!$	1	2	12	288	34560

定义 13.1.6 设 $\boldsymbol{A}$ 是$[1,n]$上的 n 阶拉丁方，其主对角线与

次对角线上的元素分别两两相异，则称 $\boldsymbol{A}$ 为 $\boldsymbol{n}$ **阶对角线拉丁方**. 并有以下定理.

定理 13.1.7 设 $n>1$，则存在 n 阶对角线拉丁方的充要条件是 $n\neq 2,3$.

13.2 正交设计与正交试验设计

13.2.1 正交拉丁方与正交表

定义 13.2.1 设基集为 $S=[1,n]$，$\boldsymbol{A}=(a_{ij})_{n\times n}$，$\boldsymbol{B}=(b_{ij})_{n\times n}$ 是 S 上的两个 n 阶拉丁方，若每一个有序对 $(i,j)(1\leqslant i\leqslant n,1\leqslant j\leqslant n)$ 都在集合

$$M=\{(a_{ij},b_{ij})\mid i,j=1,2,\cdots,n\}$$

中出现，即满足条件 $M=S\times S$，则称 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 是**正交的**(orthogonal).

若有拉丁方：$\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_s$，它们两两正交，则称它们为**正交拉丁方组**(orthogonal latin squares).

定理 13.2.2 正交拉丁方组的存在性 关于正交拉丁方组存在的条件有以下结果：

(1) 不存在 2 阶和 6 阶的一对正交拉丁方.

(2) 对任何 $n\neq 2,6$ 的正整数，都存在一对 n 阶正交拉丁方.

定义 13.2.3 设 $n\geqslant 2$，$\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_s$ 为一组 n 阶正交拉丁方，则 $s\leqslant n$. 当 $s=n-1$ 时，称 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_{n-1}$ 为 n 阶**完备的正交拉丁方组**. 且当 $n=p^r$，p 为素数时，存在 n 阶正交拉丁方的完备组(见定理 13.2.4).

定理 13.2.4 正交拉丁方的最大个数 设 n 的标准素因子分解式为 $n=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$，$N(n)$ 为两两正交的拉丁方的最大个数，则有

(1) 当 $n=p^r$ 时，$N(p^r)=p^r-1$.

(2) $N(n)\geqslant N_0(n)=\min\limits_{1\leqslant i\leqslant s}(p_i^{r_i}-1)$.

(3) 当 $n\not\equiv 2(\mathrm{mod}4)$时，至少存在一对 n 阶正交拉丁方.

(4) 若 $N(n)\geqslant 2$,则 $N(3n+1)\geqslant 2$.

(5) 若 $t\geqslant 2$,则有 $N(4t+2)\geqslant 2$.

(6) $N(n)$的一般计算方法尚未解决.

定理 13.2.5 设 S 是 n 个元素，A 是 S 上一个 $n^2\times m$ 的阵列，若 A 的任意两列是正交的：任意两列形成的有序对集恰等于 $S\times S$. 则称 A 是 S 上的一个 $n^2\times m$ **正交表**(orthogonal layout)，记作 $OA(n,m)$. 正交表 OA 有以下性质.

定理 13.2.6 存在 s 个 n 阶正交拉丁方组的充要条件是存在正交表 $OA(n,s+2)$.

13.2.2 正交试验设计与试验用正交表

设要做配方试验. 共有 m 个参数，称为因子. 每个参数(因子)有 t 个不同的取值，t 称为水平数. 用枚举法，共需做 t^m 次试验. 可以把这 t^m 次试验的参数值想象为 t 维空间中的一个超立方体上的格子点. 如果能设计一个试验方案，只取这个超立方体上一些有代表性的格子点，且这些代表点在超立方体中的分布有一定的均匀性，这种设计试验的方法称为“试验设计”. 采用不同的代表性或均匀性，就得到不同的试验设计方法. 正交试验设计的规则是：任何两个参数的两个水平，在试验中恰有一次搭配.

设共做 N 次试验($N\ll t^m$)，可把每一次试验对应的参数取值写成一行(每个参数取值范围为 $1,2,\cdots,t$)，得到一个 $N\times m$ 的阵列，记作 $L_N(t^m)$，称为一个 m 个因子 t 水平共做 N 次试验的正交表. 因而 OA 正交表可表为

$$OA(n,s+2)=L_{n^2}(n^{(s+2)}),$$

即利用 $OA(n,s+2)$ 可安排 $s+2$ 个因子 n 水平的正交试验，共需做 n^2 次试验. 显然，当 n 适当大时有 $n^2 \ll (s+2)^n$. 即正交试验法可大大减少试验次数.

13.2.3 正交试验表的一般形式

在一般情况下，每个因子的水平数可以不同，设有 m_1 个因子的水平数均为 t_1，m_2 个因子的水平数均为 t_2，…，m_k 个因子的水平数均为 t_k，共做 N 次试验，这样的正交试验表记作

$$L_N(t_1^{m_1} \times t_2^{m_2} \times \cdots \times t_k^{m_k}).$$

构造一般的正交表的工作十分复杂，已有一些现成的表可查用. 对于等水平的正交试验表可用正交拉丁方组来构造.

正交设计指的是构造正交拉丁方组的方法；而正交试验设计指的是构造正交试验表的方法.

13.2.4 正交拉丁方组的构造方法

设 $n=p^r$，p 为素数. 算法步骤如下：

(1) 设 $F=GF(p^r)$ 为 p^r 阶有限域，作出 F 的加法表与乘法表.

(2) 令 $y=mx+k$，对每一个 $m\neq 0$ 作下表：

$y=mx+k$ \ k / x	0	1	……
0			
1		$a_{xk}=mx+k$	
⋮			
⋮			

得到一个 $n\times n$ 的阵列记作 $L(m)$，就是一个拉丁方，共可得到 $n-1$ 个拉丁方：$\mathbf{A}_1,\mathbf{A}_2,\cdots,\mathbf{A}_{n-1}$，它们构成完备的正交的拉丁方组. 且具有以下性质：它们的首行都相同，则 $\mathbf{A}_i$ $(i\geqslant 2)$的第 $2\sim n$ 行是 $\mathbf{A}_1$ 的第 $2\sim n$ 行的一个行置换. 因此，实际计算时，只需计算 $\mathbf{A}_1$ 及每个 $\mathbf{A}_i$ $(i\geqslant 2)$的第 1 列元素. 其余元素可从 $\mathbf{A}_1$ 得到.

例 13.2.7 构造 4 阶正交拉丁方完备组及相应的正交表.

解 (1) 设 $F=GF(2^2)$，作出 F 的元素的加法表与乘法表. 方法如下：

在 $\mathbf{Z}_p$ 上选一个 2 次本原多项式：$m(x)=x^2+x+1$，设 α 是该本原多项式的根，则 $F=\{0,1,\alpha,\alpha^2\}$，其加法表与乘法表分别如下：

$+$ (x \ y)	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\times$ (x \ y)	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

(2) 设 $y=mx+l,m\in F^*$

取 $m=1,y=x+l$，作下表：

$x \backslash y$ (l)	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

分别用 1,2,3,4 代表 $0,1,\alpha,\alpha^2$,得到以下的拉丁方:

$$\boldsymbol{L}_1=\begin{bmatrix}1&2&3&4\\2&1&4&3\\3&4&1&2\\4&3&2&1\end{bmatrix}.$$

取 $m=\alpha$,由 $y=\alpha x$ 求得第 1 列元素为 $0,\alpha,\alpha^2,1$,即 1,3,4,2,由 $\boldsymbol{L}_1$ 作行置换,得到第二个拉丁方:

$$\boldsymbol{L}_2=\begin{bmatrix}1&2&3&4\\3&4&1&2\\4&3&2&1\\2&1&4&3\end{bmatrix}.$$

取 $m=\alpha^2$,由 $y=\alpha^2 x$ 求得第 1 列元素为 $0,\alpha^2,1,\alpha$ 即 1,4,2,3,由 $\boldsymbol{L}_1$ 作行置换得

$$\boldsymbol{L}_3=\begin{bmatrix}1&2&3&4\\4&3&2&1\\2&1&4&3\\3&4&1&2\end{bmatrix}$$

共得到 $\boldsymbol{L}_1,\boldsymbol{L}_2,\boldsymbol{L}_3$ 三个拉丁方,构成拉丁方完备组.

(3) 由两个初始列及 $\boldsymbol{L}_1,\boldsymbol{L}_2,\boldsymbol{L}_3$,可得正交表 $OA(4,5)$:

$$OA(4,5) = (\boldsymbol{L}_{16}(4^5)) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 & 2 \\ 1 & 3 & 3 & 3 & 3 \\ 1 & 4 & 4 & 4 & 4 \\ 2 & 1 & 2 & 3 & 4 \\ 2 & 2 & 1 & 4 & 3 \\ 2 & 3 & 4 & 1 & 2 \\ 2 & 4 & 3 & 2 & 1 \\ 3 & 1 & 3 & 4 & 2 \\ 3 & 2 & 4 & 3 & 1 \\ 3 & 3 & 1 & 2 & 4 \\ 3 & 4 & 2 & 1 & 3 \\ 4 & 1 & 4 & 2 & 3 \\ 4 & 2 & 3 & 1 & 4 \\ 4 & 3 & 2 & 4 & 1 \\ 4 & 4 & 1 & 3 & 2 \end{bmatrix}$$

算法 13.2.8　$n=p, OA(p,p+1)=L_{p^2}(p^{p+1})$的构造方法

这是(13.2.4)的特殊情况：$r=1$，它的构造方法最为简单. 首先写出 $\boldsymbol{L}_1$，它是以下的循环阵列：

$$\boldsymbol{L}_1 = \begin{bmatrix} 0 & 1 & 2 & \cdots & \cdots & p-1 \\ 1 & 2 & 3 & \cdots & p-1 & 0 \\ 2 & 3 & \cdots & p-1 & 0 & 1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ p-1 & 0 & 1 & \cdots & p-3 & p-2 \end{bmatrix}$$

$\boldsymbol{L}_m$ ($m=2,3,\cdots,p-1$) 的第 1 列为 $0, m, 2m, \cdots, (p-1)m \pmod p$. 然后从 $\boldsymbol{L}_1$ 中找到第一个元素相同的行，由此得 $OA(p,p+1)$的构造如下.

$OA(p,p+1)$：

第 1,2 列为初始列：

$$0,0,\cdots,0,1,1,\cdots,1,\cdots\cdots,p-1,p-1,\cdots,p-1$$

$$1,2,\cdots,p-1,1,2,\cdots,p-1,\cdots\cdots,1,2,\cdots,p-1$$

第 $3\sim p+1$ 列分别为 $\boldsymbol{L}_1,\boldsymbol{L}_2,\cdots,\boldsymbol{L}_{p-1}$ 的元素按行排列.

算法 13.2.9 $l\times m$ 阶正交拉丁方组的构造方法 设 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_s$ 为 l 阶正交拉丁方组，$\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_s$ 为 m 阶正交拉丁方组，则

$\boldsymbol{A}_1*\boldsymbol{B}_1,\boldsymbol{A}_2*\boldsymbol{B}_2,\cdots,\boldsymbol{A}_s*\boldsymbol{B}_s$ 为 lm 阶正交拉丁方组，其中 $\boldsymbol{A}*\boldsymbol{B}$ 的意义为

设 $\boldsymbol{A}=(a_{ij})_{l\times l}$，$\boldsymbol{B}=(b_{ij})_{m\times m}$ 则

$$\boldsymbol{A}*\boldsymbol{B}=\begin{bmatrix}(a_{11},b_{11}) & & (a_{11},b_{1m}) & \cdots & (a_{1l},b_{11}) & \cdots & (a_{1l},b_{1m})\\ \vdots & & \vdots & & \vdots & & \vdots\\ (a_{11},b_{m1}) & \cdots & (a_{11},b_{mm}) & \cdots & (a_{1l},b_{m1}) & & (a_{1l},b_{mm})\\ \vdots & & \vdots & & \vdots & & \vdots\\ (a_{l1},b_{11}) & & (a_{l1},b_{1m}) & \cdots & (a_{ll},b_{11}) & \cdots & (a_{ll},b_{1m})\\ \vdots & & \vdots & & \vdots & & \vdots\\ (a_{l1},b_{m1}) & \cdots & (a_{l1},b_{mm}) & \cdots & (a_{ll},b_{m1}) & \cdots & (a_{ll},b_{mm})\end{bmatrix}.$$

例 13.2.10 构造 12 阶正交拉丁方组

由于 $12=3\times4$，3 阶正交拉丁方组有两个：

$$\boldsymbol{A}_1=\begin{bmatrix}a_1 & a_2 & a_3\\ a_2 & a_3 & a_1\\ a_3 & a_1 & a_2\end{bmatrix},\qquad \boldsymbol{A}_2=\begin{bmatrix}a_1 & a_2 & a_3\\ a_3 & a_1 & a_2\\ a_2 & a_3 & a_1\end{bmatrix}.$$

4 阶正交拉丁方组虽然有 3 个(见例 13.2.7)，由上述方法只能构造出两个正交的 12 阶拉丁方，因而可任取两个正交的 4 阶拉丁方，例如取 $\boldsymbol{B}_1$ 为例 13.2.7 中的 $\boldsymbol{L}_1$，$\boldsymbol{B}_2$ 为例 13.2.7 中的 $\boldsymbol{L}_2$，并记作

$$B_1 = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ b_2 & b_1 & b_4 & b_3 \\ b_3 & b_4 & b_1 & b_2 \\ b_4 & b_3 & b_2 & b_1 \end{bmatrix},$$

$$B_2 = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ b_3 & b_4 & b_1 & b_2 \\ b_4 & b_3 & b_2 & b_1 \\ b_2 & b_1 & b_4 & b_3 \end{bmatrix}.$$

令$(a_1, b_1)=1$, $(a_1, b_2)=2$, $(a_1, b_3)=3$, $(a_1, b_4)=4$,
$(a_2, b_1)=5$, $(a_2, b_2)=6$, $(a_2, b_3)=7$, $(a_2, b_4)=8$,
$(a_3, b_1)=9$, $(a_3, b_2)=10$, $(a_3, b_3)=11$, $(a_3, b_4)=12$.

则得

$$C_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 \\ 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 1 & 2 & 3 & 4 \\ 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 2 & 1 & 4 & 3 \\ 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 & 3 & 4 & 1 & 2 \\ 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 & 4 & 3 & 2 & 1 \\ 9 & 10 & 11 & 12 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 10 & 9 & 12 & 11 & 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 11 & 12 & 9 & 10 & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 12 & 11 & 10 & 9 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{bmatrix}.$$

C_2 的第 1 行与 C_1 相同. 第 1 列元素为：1,3,4,2,9,11,12,10,5,7,8,6,各行的元素为 C_1 中第 1 个元素相同的对应行.

算法 13.2.11　任意 n 阶正交拉丁方组的构造方法

设 $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$, $p_1, p_2, \cdots, p_s$ 为互不相同的素数,

$r_i \geqslant 1$. 令

$$N_0(n) = \min_{1 \leqslant i \leqslant s}(p^{r_i} - 1),$$

则由 13.2.4 可构造出 $N_0(n)$个相互正交的 n 阶拉丁方.

13.2.5 应用

例 13.2.12 试验田问题 1 要在一块正方形的试验田上试验 3 个品种的小麦,为了减少土质的影响,把试验田等分成 3 横条 3 竖条,共 9 块,做试验安排如下:每个品种在每一个横条或每一个竖条上恰出现一次,这样所得的试验安排就是一个 3 阶拉丁方.

例 13.2.13 试验田问题 2 若有 n 种肥料,n 种水质,要试验它们对小麦产量的效果. 为了减少土地的影响,把正方形的试验田等分为 n 个横条与 n 个竖条共 n^2 个小块,按以下规则对这 n^2 个小块上的小麦做试验:

(1) 每种肥料或每种水质在每一横条或每一竖条上恰出现一次;

(2) 每种肥料与每种水质在 n^2 个小块上恰有一次搭配(又称相遇).

设 $\boldsymbol{A}$ 是由 n 种肥料组成的拉丁方,$\boldsymbol{B}$ 是由 n 种水质组成的拉丁方,并使 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 正交,则(a_{ij}, b_{ij}), $i,j=1,2,\cdots,n$ 就是第(i,j)小块土地上对应的肥料与水质.

例 13.2.14 配方问题 设用 k 种原料来配制一种饮料或药剂,每一种原料有 n 种剂量,要试验如何配制得到最好的效果. 用枚举法要做 n^k 次试验(设 $k>2$). 为了减少试验次数,只要求试验满足以下规则:任何两种原料的两种剂量在试验中恰有一次搭配. 可以认为这样的试验方案具有一定的代表性与遍历性,是比较合理的. 这可用 k 个正交的 n 阶拉丁方 $\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_k$ 来实现. 由 $\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_k$ 构成正交表 $OA(n,k)$,它的每一列代表某一种原料的剂量,每一行代表一次试验所对应的每种原料的剂量. 共需

做 n^2 次试验，当 $k>2$ 时，减少了试验次数.

正交表 OA 可直接用于等水平数的试验设计. 对于非等水平的试验问题，则需要用"正交试验表"来安排试验，可查阅有关正交试验设计的书.

13.3 平衡不完全区组设计

定义 13.3.1 设 X 为 v 元集合，k,λ 为正整数，若区组设计 $\mathscr{B}=\{B_1,B_2,\cdots,B_b\}$ 满足：

(1) 对任意 $B_i\in\mathscr{B}$，有 $|B_i|=k$；

(2) 对任意 $x\in X$，x 恰属于 r 个区组，r 称 x 在 $\mathscr{B}$ 中的出现数.

(3) 对任意两个元素 $x,y\in X$，同时含有 x 和 y 的区组数都等于 λ，称 λ 为 x,y 的相遇数.

则称 $\mathscr{B}$ 是 X 上的一个 (b,v,r,k,λ) **平衡不完全区组设计**(balanced incomplete block design)，简称 (b,v,r,k,λ)，$-$BIBD，(b,v,r,k,λ) 称为该设计的**类型**.

平衡是指等出现数及等相遇数. 不完全是指：$B_i\not\subseteq X$，或 $k<v$.

每个区组内的元素是无序的，每个区组内元素的个数相等，称为**等长**. 所以 BIBD 是等长无序的出现数与相遇数均相等的区组设计.

例 13.3.2 $(b=12,v=9,r=4,k=3,\lambda=1)-$BIBD：

$B_1=\{1,2,3\}$，$B_2=\{4,5,6\}$，$B_3=\{7,8,9\}$，

$B_4=\{1,4,7\}$，$B_5=\{2,5,8\}$，$B_6=\{3,6,9\}$，

$B_7=\{1,5,9\}$，$B_8=\{2,6,7\}$，$B_9=\{3,4,8\}$，

$B_{10}=\{1,6,8\}$，$B_{11}=\{2,4,9\}$，$B_{12}=\{3,5,7\}$.

定理 13.3.3 BIBD 的参数的性质 设存在一个 $(b,v,r,k,$

λ)－BIBD，则有

(1) $r(k-1)=\lambda(v-1)$；

(2) $bk=vr$；

(3) $\lambda(v-1)\equiv 0(\bmod(k-1))$；

(4) $\lambda v(v-1)\equiv 0(\bmod k(k-1))$；

(5) 当 $1<k<v$ 有 $b\geqslant v$ 或 $\lambda(v-1)\geqslant k(k-1)$.

例 13.3.4　一些特殊情况的 BIBD：

(1) 不存在 $v=16,k=6,\lambda=1$ 及 $v=21,k=6,\lambda=1$ 的 BIBD.

(2) $k=1$ 时，由 X 的任意多个 1 元子集构成的区组设计都是 BIBD，设计类型为 $(rv,v,r,1,0)$.

(3) $k=2$ 时，$\mathscr{B}$ 由 X 中的所有 2 元子集重复 λ 次构成，设计类型为 $\left(\lambda\frac{v(v-1)}{2},v,\lambda(v-1),2,\lambda\right)$.

(4) $k=v$ 时，$\mathscr{B}$ 由 λ 个 X 组成.

(5) $k=v-1>2$ 时，当 $(v-2)\nmid\lambda$，不存在 $k=v-1$ 的 BIBD；当 $(v-2)\mid\lambda$，存在由 X 的所有 $(v-1)$-子集重复 $\lambda/(v-2)$ 次所构成的 BIBD，且是唯一的. 设计类型为

$(vt,v,(v-1)t,v-1,(v-2)t)$，其中 t 为任一整数.

(6) $k=v-2>2$ 时，当 $\binom{v-2}{2}\nmid\lambda$，不存在 $k=v-2$ 的 BIBD；当 $\binom{v-2}{2}\Big|\lambda$ 时，存在由 X 的所有 $(v-2)$-子集重复 $\lambda\Big/\binom{v-2}{2}$ 次构成的 BIBD，且是唯一的. 设计类型为 $\left(t\,\frac{v(v-1)}{2},v,t\,\frac{(v-1)(v-2)}{2},v-2,t\,\frac{(v-2)(v-3)}{2}\right)$，其中 t 为任一正整数.

定义 13.3.5　设 X 为 v 元集合，区组设计 $\mathscr{B}=\{B_1,B_2,\cdots,B_b\}$，满足：

(1) 设 K 是正整数集合，$\forall B_i\in\mathscr{B}$ 有 $|B_i|\in K$；

(2) $\forall x,y\in X$ 且 $x\neq y$，它们的相遇数为常数 λ.

则称 $\mathscr{B}$ 为不等长平衡区组设计，习惯上称为**成对（或不等长）平衡设计**，记作 (v,k,λ)-设计.

定义 13.3.6 设 X 为 v 元集合，$\{X_1,X_2,\cdots,X_t\}$ 是 X 的一个划分，每一个子集 X_j 称为类. 区组设计 $\mathscr{B}=\{B_1,B_2,\cdots,B_b\}$ 满足：

(1) 有正整数集合 K，使 $K=\{k\,|\,k=|B_i|,i=1,2,\cdots,b\}$；

(2) 有正整数集合 M，使 $M=\{m\,|\,m=|X_j|,j=1,2,\cdots,t\}$；

(3) $\forall x,y\in X$ 且 $x\neq y$，有

当 x,y 属于同一类时，相遇数为 0；

当 x,y 属于不同类时，相遇数为常数 λ.

则称 $\mathscr{B}$ 为**可分类区组设计**，记作 (v,K,λ,M)-设计. $\{|X_1|,|X_2|,\cdots,|X_t|\}$ 称为该可分类设计的分类型式.

这种设计的特点是基集划分为类；区组不等长；两个元素只有属于不同类时才等于非零常数 λ.

定义 13.3.7 设 X 为 v 元集合，划分为类：$\{X_1,X_2,\cdots,X_t\}$，区组设计 $\mathscr{B}=\{B_1,B_2,\cdots,B_b\}$ 满足：

(1) 每个区组长度相等：$\forall B_i\in\mathscr{B}$ 有 $|B_i|=k\geqslant 2$；

(2) 每类元素个数相同：$\forall X_i$ 有 $|X_i|=m$；

(3) 同类元素的相遇数为 0，不同类元素的相遇数为常数 λ.

则称 $\mathscr{B}$ 为 (v,k,λ,m)-**横截设计**(transverse design).

这种区组设计的特点是，分类等"长"为 m，区组等长为 k，只有不同类元素的相遇数为非零常数 λ.

定理 13.3.8 横截设计的性质 设 $\mathscr{B}$ 是 (b,v,k,λ,m)-横截设计，则有

(1) 分类数与区组长相等：$t=k$.

(2) $\forall B_i\in\mathscr{B},X_j$ 有 $|B_i\cap X_j|=1$，即任一区组由每类取一个元素组成.

(3) $b=\lambda m^2$.

(4) $r=\lambda m$,每个元素的出现数为 λm.

定理 13.3.9 横截设计与正交设计的关系 存在 $\lambda=1$ 的 $(v,b,k,1,m)$-横截设计的充要条件是存在一个 k 列的 m 阶正交表 $OA(m,k)$.

13.4 三元系

13.4.1 三元系与 Steiner 三元系

$k=3$ 的不完全平衡区组设计,即 $(v,b,r,3,\lambda)$-设计,称为**三元系**(triple system)或**三连系**. 当 $\lambda=1$ 时,即 $(v,b,r,3,1)$-设计,称为 **Steiner 三元系**(Steiner triple system).

这种设计是 k 值最小的非平凡的 (v,b,r,k,λ)-BIBD.

13.4.2 Steiner 三元系的性质

定理 13.4.1 参数关系 (v,b,r)-Steiner 三元系满足

$$r=\frac{v-1}{2},\ b=\frac{v(v-1)}{6}.$$

定理 13.4.2 存在定理 (Steiner)三元系 (v,b,r) 存在的充分必要条件为

$$v\equiv 1,\ 或\ 3(\mathrm{mod}\ 6),\ v\geqslant 3.$$

例 13.4.3 (1) $v=3$ 的 Steiner 三元系存在且唯一,而且只有一个区组:$\{1,2,3\}$.

(2) $v=7$ 的 Steiner 三元系存在且唯一,为$\{1,2,3\}$,$\{1,4,5\}$,$\{1,6,7\}$,$\{2,4,6\}$,$\{2,5,7\}$,$\{3,4,7\}$,$\{3,5,6\}$.

(3) $v=9$ 的 Steiner 三元系在同构意义下存在且唯一,为

$\{1,2,3\}$,$\{1,4,5\}$,$\{1,6,7\}$,$\{1,8,9\}$,$\{2,4,6\}$,$\{2,5,8\}$,$\{2,7,9\}$,$\{3,4,9\}$,$\{3,5,7\}$,$\{3,6,8\}$,$\{4,7,8\}$,$\{5,6,9\}$.

(4) $v=13$ 的 Steiner 三元系，互不同构的有两个：$\mathscr{B}_1$，$\mathscr{B}_2$. $\mathscr{B}_1$ 为

{1,2,3}，{1,4,5}，{1,6,7}，{1,8,9}，{1,10,11}，{1,12,13}，{2,4,6}，{2,5,7}，{2,8,10}，{2,9,12}，{2,11,13}，{3,4,8}，{3,5,12}，{3,7,11}，{4,7,9}，{4,10,13}，{4,11,12}，{5,8,11}，{6,8,12}，{6,9,11}，{7,8,13}，{7,10,12}，{3,6,10}，{3,9,13}，{5,6,13}，{5,9,10}.

$\mathscr{B}_2$ 是将 $\mathscr{B}_1$ 中的最后 4 个区组换为{3,6,13}，{3,9,10}，{5,6,10}，{5,9,13}.

(5) $v=15$ 时，共有 80 个互不同构的 Steiner 三元系，每个三元系的区组数为 35.

(6) 对一般的 $v\equiv 1$，或 3(mod6)的互不同构的 Steiner 三元系的个数问题尚未完全解决.

13.4.3 Steiner 三元系的构造方法

若存在 Steiner 三元系 $ST_1(v_1)$ 和 $ST_2(v_2)$，则存在 $ST(v_1v_2)$，且此三元系分别包含与 $ST_1(v_1)$和 $ST_2(v_2)$同构的子系. 具体构造方法如下：

设$ST_1(v_1)$的基集为 $X=\{a_1,a_2,\cdots,a_{v_1}\}$，

$ST_2(v_2)$的基集为 $Y=\{b_1,b_2,\cdots,b_{v_2}\}$.

令 $S=\{c_{ij}\mid 1\leqslant i\leqslant v_1, 1\leqslant j\leqslant v_2\}$ 为 $ST(v_1v_2)$ 的基集，$ST(v_1v_2)$的构造如下：

$\{c_{iw},c_{jx},c_{ly}\}\in ST(v_1v_2)$ 的充分必要条件为满足以下条件之一：

(1) $w=x=y$ 且$\{a_i,a_j,a_l\}\in ST_1(v_1)$；

(2) $i=j=l$ 且$\{b_w,b_x,b_y\}\in ST_2(v_2)$；

(3) $\{a_i,a_j,a_l\}\in ST_1(v_1)$且$\{b_w,b_x,b_y\}\in ST_2(v_2)$.

13.4.4 Steiner三元系大集问题

设 X 为 v 元集合，$ST_1(v)$，$ST_2(v)$是 X 上的两个 Steiner 三元系，若它们没有公共的区组，就称它们是不相交的. 设 $D(v)$是 v 元集 X 上的两两不相交的 Steiner 三元系的最大个数，则

$$D(v) \leqslant \frac{\binom{v}{3}}{\frac{v(v-1)}{6}} = v-2.$$

若存在 $v-2$ 个两两不相交的 Steiner 三元系：$ST_1(v)$，$ST_2(v)$，…，$ST_{v-2}(v)$，则称它是一个 **Steiner 三元系大集**(set of steiner triple systems). 确定存在大集的 v 值问题，称为 Steiner 三元系大集问题. 并有以下结果.

定理 13.4.4 Steiner三元系大集定理/陆家羲定理 对所有适合 $v\equiv 1$，或 3(mod 6)且 $v>7$ 的 v 值，除 6 个可能的例外值：141，283，501，789，1501，2365，都存在 Steiner 三元系大集.

13.4.5 应用

例 13.4.5 Kirkman 女生问题 (见 7.9 节)15 名女生，每天 3 人一组出去散步，女教师安排了一个分组方案，使 7 天中任两个女生恰分在同一组一次. 这是个 Steiner 三元系的问题，由 13.4.2 节区组数为 $b=35$，出现数 $r=7$，因而这 35 个区组可分成 7 大组，使每个人都出现在每个大组中.

Kirkman 给出的解答为

星期日 {1,2,3}，{4,8,12}，{5,10,15}，{6,11,13}，{7,9,14}；
星期一 {1,4,5}，{2,8,10}，{3,13,14}，{6,9,15}，{7,11,12}；
星期二 {1,6,7}，{2,9,11}，{3,12,15}，{4,10,14}，{5,8,13}；
星期三 {1,8,9}，{2,12,14}，{3,5,6}，{4,11,15}，{7,10,13}；

星期四　$\{1,10,11\},\{2,13,15\},\{3,4,7\},\{5,9,12\},\{6,8,14\}$;
星期五　$\{1,12,13\},\{2,4,6\},\{3,9,10\},\{5,11,14\},\{7,8,15\}$;
星期六　$\{1,14,15\},\{2,5,7\},\{3,8,11\},\{4,9,13\},\{6,10,12\}$.

这样的安排方案有很多个,两两不相交的方案有 13 个,两两不同构的方案有 80 个.

例 13.4.6　饲料试验(Kirkman 女生问题的其他形式)　设有 15 种饲料,要从中选出 3 种饲料的最佳搭配. 如果用枚举法,需做 $\binom{15}{3}=455$ 次试验. 利用 Steiner 三元系设计可减少试验次数且其结果具有一定的可靠性. 具体安排如下:

试验分 7 阶段进行,每阶段 5 天,每天喂养一个 3 种饲料的搭配,并要求满足以下条件:(1) 每种饲料在每个阶段恰用过一次;(2) 每两种饲料在全部试验中恰搭配过一次. 该问题的解就是 Kirkman 女生问题的解.

例 13.4.7　配方问题　今有 t 种原料,每种原料有 m 种剂量,要配制混合物,选择最佳配方. 设每种原料的剂量的集合为 $X_i, i=1,2,\cdots,t, X=\{X_1,X_2,\cdots,X_t\}$,区组设计 $\mathscr{B}=\{B_1,B_2,\cdots,B_b\}$ 满足

(1) $|B_j|=t, j=1,2,\cdots,b$;

(2) 每种原料在每个区组中恰出现一次;

(3) 每两种原料的任两种剂量在 $\mathscr{B}$ 中恰搭配(相遇)λ 次.

因而 $\mathscr{B}$ 是一个(tm,b,t,λ,t)-横截设计(见定义 13.3.7).

代数结构与泛代数

14 半群与群

14.1 引言

本篇论述的代数结构(系统)是指具有若干个代数运算的集所构成的数学系统,它们有半群、群、环、域、模、代数、范畴、函子、泛代数等等.

14.2 半群的定义及例子

半群是仅含一个二元运算的代数结构,它在自动机与形式语言理论中有广泛的应用.

定义 14.2.1 设$\circ$是集 S 上的一个二元运算,若满足结合律:

对于$\forall a,b,c\in S$ 都有$(a\circ b)\circ c=a\circ(b\circ c)$,则称$\langle S;\circ\rangle$是一个**半群** semi group.

定义 14.2.2 设$\langle S;\circ\rangle$是半群,若运算$\circ$满足交换律,则称$\langle S;\circ\rangle$是**交换半群**(commutative semigroup)或 Abel **半群**(Abel semingroup).

定义 14.2.3 设$\langle S;\circ\rangle$是半群,若存在元素 $e_l\in S(e_r\in S)$,对于$\forall a\in S$ 都有

$$e_l \circ a = a \quad (a \circ e_r = a),$$

则 $e_l(e_r)$称为$\langle S;\circ\rangle$的**左(右)单位元**,(left(right)identify),简称**左(右)单元**.

若$\langle S;\circ\rangle$的一个元素既是左单元,又是右单元,则称它为$\langle S;\circ\rangle$的**单位元**(identity),或**单元**,记作 e.

定理 14.2.4 若半群$\langle S;\circ\rangle$存在左单元 e_l 和右单元 e_r,则它们都是唯一的,而且二者相等.

定义 14.2.5 具有单元的半群称为**单元半群**(monoid).

例 14.2.6 仍用$+$、$\cdot$、$-$表示数的加法、乘法和减法,则$\langle \mathbf{N};+\rangle$,$\langle \mathbf{N};\cdot\rangle$,$\langle \mathbf{Z};+\rangle$,$\langle \mathbf{Z};\cdot\rangle$,$\langle \mathbf{Q};+\rangle$,$\langle \mathbf{Q};\cdot\rangle$,$\langle \mathbf{R};+\rangle$,$\langle \mathbf{R};\cdot\rangle$,$\langle \mathbf{C};+\rangle$,$\langle \mathbf{C};\cdot\rangle$都是半群.又因为它们的运算满足交换律,而且它们分别以数 0 或 1 作为单元,所以它们都是交换单元半群.

但$\langle \mathbf{Z};-\rangle$不是半群,因为整数的减法"$-$"不满足结合律.

例 14.2.7 设 $\mathbf{Z}_n$ 是模 n 同余类集,$+$、$\cdot$分别为同余类的加法和乘法,则$\langle \mathbf{Z}_n;+\rangle$,$\langle \mathbf{Z}_n;\cdot\rangle$都是交换单元半群,它们的单元分别是同余类 C_0 及 C_1.

例 14.2.8 设 A 是任一集,它的幂集 $\mathcal{P}(A)$关于集的并与交两种运算所构成的两个结构$\langle \mathcal{P}(A);\cup\rangle$及$\langle \mathcal{P}(A);\cap\rangle$都是交换单元半群,它们的单元分别是空集$\varnothing$及集 A.

例 14.2.9 设 X 是任一集,$X^X=\{\varphi \mid X\to X\}$是 X 到它自身的所有映射(称为 X 的变换)构成的集,则 X^X 对于映射的复合运算"$\circ$"所构成的代数结构$\langle X^X;\circ\rangle$是一个单元半群,它的单元是恒等变换.

然而这个单元半群不是交换半群.

特例:设 $X=\{0,1\}$,则 X^X 含有以下 4 个变换:

ε: $0\mapsto 0, 1\mapsto 1$;

α: $0 \mapsto 0, 1 \mapsto 0$;

β: $0 \mapsto 1, 1 \mapsto 0$;

γ: $0 \mapsto 1, 1 \mapsto 1$.

$\langle X^X; \circ \rangle$的运算如表 14.1，由表易见它的运算是不满足交换律的.

表 14.1

$\circ$	ϵ	α	β	γ
ϵ	ϵ	α	β	γ
α	α	α	α	α
β	β	γ	ϵ	α
γ	γ	γ	γ	γ

例 14.2.10 整数集 $\mathbf{Z}$ 上运算$\circ$规定为：

对于 $\forall x, y \in \mathbf{Z}, x \circ y = 6 - 2x - 2y + xy$.

则$\langle \mathbf{Z}; \circ \rangle$是一个交换单元半群，其单元是 3.

例 14.2.11 设 Σ 是由一些字符或数码组成的字母表(alphabet)（如英文字母表 $\Sigma_1 = \{a, b, c, \cdots, x, y, z\}$ 及二进制数码表 $\Sigma_2 = \{0, 1\}$），Σ^+ 是由 Σ 的字母组成的（不含空串的）有限字符串（如 $aab, abbba, boy$ 等都是 Σ_1 的字符串，而 00,010,110001 等都是 Σ_2 的字符串）的集，Σ^* 是由 Σ 的所有字符串与不含字符的**空串**Λ构成的集，其上定义的**邻接运算**(concatenation/juxtaposition) 为

若 $\alpha, \beta \in \Sigma^+ (\Sigma^*)$，则 $\alpha \circ \beta = \alpha\beta$.

（例如在 Σ^+ 上 $aab \circ abbba = aababbba$).

可以证明，$\langle \Sigma^+, \circ \rangle$ 构成一个半群. $\langle \Sigma^*, \circ \rangle$ 构成一个单元半群，其单元是空串 Λ.

14.3 半群的基本性质

14.3.1 半群中元素的表示法

为了简便，今后半群中的运算符号“$\circ$”按通常写法记作 · 或 +，并分别读为乘法或加法；半群$\langle S; \circ \rangle$及单元半群$\langle M; \circ \rangle$也仅用它们的基集 S 及 M 表示.

由于半群的乘法满足结合律，因此可递归地给出半群及单元半群中元素幂的概念.

定义 14.3.1 设 S 是一个半群，$a\in S$，$n\in \mathbf{N}^+$，则 a 的 **n 次幂**(power)为：

(1) $a^1=a$，

(2) $a^{n+1}=a\cdot a^n$.

定义 14.3.2 设 M 是一个单元半群，$a\in M$，$n\in \mathbf{N}$，则 a 的 n 次幂为：

(1) $a^0=e$，

(2) $a^{n+1}=a\cdot a^n$.

定理 14.3.3 对于半群 S 中的 $\forall a\in S$ 及 $\forall m,n\in \mathbf{N}^+$，都有 $a^m\cdot a^n=a^{m+n}$.

定理 14.3.4 对于单元半群 M 中的 $\forall a\in M$ 及 $\forall m,n\in \mathbf{N}$，都有 $a^m\cdot a^n=a^{m+n}$.

定理 14.3.5 在交换半群 S 中，对于 $\forall a,b\in S$ 及 $\forall m\in \mathbf{N}^+$ 成立：$(a\cdot b)^m=a^m\cdot b^m$.

定理 14.3.6 在交换的单元半群 M 中，对于 $\forall a,b\in M$ 及 $\forall m\in \mathbf{N}$ 成立：$(a\cdot b)^m=a^m\cdot b^m$.

定义 14.3.7 半群 S 的元素 a，若 $a^2=a$，则称它为 S 的**幂等元**(idempotent element).

例 14.3.8 (1) 任一单元半群的单元 e 都是它的幂等元.

(2) 单元半群 $\langle \mathscr{P}(A),\cup\rangle$ 及 $\langle \mathscr{P}(A),\cap\rangle$ 的任一子集 B 都是它们的幂等元. 因为集的运算法则有 $B\cup B=B$，$B\cap B=B$(见例 14.2.8).

(3) 半群 $\langle X^X,\circ\rangle$ 的元 ϵ,α,γ 都是幂等元，只有 β 不是幂等元(见例 14.2.9).

定义 14.3.9 半群 S 的一个元素 $0_l(0_r)$，若对于 $\forall x\in S$：

$0_l \cdot x = 0_l$ ($x \cdot 0_r = 0_r$)，则称为 S 的**左(右)零元**，(left, right zero).

若 S 的一个元素 0 既是左零元又是右零元，则称 0 是 S 的**零元**(zero).

例 14.3.10 (1) 在例 14.2.8 中，集 A 是 $\langle \mathscr{P}(A), \cup \rangle$ 的零元，而空集 $\varnothing$ 是 $\langle \mathscr{P}(A), \cap \rangle$ 的零元.

(2) 在例 14.2.9 中，α 及 γ 都是 $\langle X^X, \circ \rangle$ 的左零元，它没有右零元因而也没有零元.

定理 14.3.11 若半群(单元半群)有一个左零元 0_l 及一个右零元 0_r，则它们都是唯一的，且二者相等.

14.3.2 循环半群

定义 14.3.12 若半群 S 的每个元素都是它的某个元素 c 的正整数幂，即

$$S = \{c^r \mid r \in \mathbf{N}^+\},$$

则称为循环半群(cyclic semigroup). 并称半群 S 是由元素 c 生成的，用 $S=(c)$ 表示，c 称为 S **的生成元**(generator of S).

定义 14.3.13 若单元半群 M 的每个元素都是它的某个元素 c 的非负整数幂，即

$$M = \{c^n \mid n \in \mathbf{N}\},$$

则称 M 为循环单元半群(cyclic monoid)，并称 M 是由元素 c 生成的，用 $M=(c)$ 表示，c 称为 M 的**生成元**.

例 14.3.14 设 $A=\{0,1,2,3\}$，变换 $\varphi: A \mapsto A$ 的对应法则是：

$$\varphi: 0 \mapsto 1,\ 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1.$$

则 φ 的前 4 个方幂 $\varphi^0=\varepsilon, \varphi^1=\varphi, \varphi^2=\varphi\circ\varphi, \varphi^3=\varphi\circ\varphi^2$ 完全相异，但 $\varphi^4=\varphi$. 此时 $M=\{\varepsilon,\varphi,\varphi^2,\varphi^3\}$ 关于映射的复合"$\circ$"作成一个循环单元半群(φ). 其乘法如表 14.2.

表 14.2

$\circ$	ε	φ	φ^2	φ^3
ε	ε	φ	φ^2	φ^3
φ	φ	φ^2	φ^3	φ
φ^2	φ^2	φ^3	φ	φ^2
φ^3	φ^3	φ	φ^2	φ^3

例 14.3.15 非负整数集 **N** 关于数的加法构成一个循环单元半群，其单元是 0，其生成元是 1：$\mathbf{N}=(1)$. 它没有零元.

N 关于数的乘法虽然构成一个单元是 1、零元是 0 的单元半群，但却不是循环半群，因为不存在一个整数 c 能使 **N** 的每个数表成 c 的非负整数次幂.

定理 14.3.16 循环(单元)半群是交换半群.

定理 14.3.17 (1) 有限循环半群至少包含一个幂等元.

(2) 有限循环单元半群恰好包含一个单元 e 以外的幂等元.

(3) 设 M 是一个有限单元半群，则对于 $\forall x \in M$ 及某个$n \in \mathbf{N}^+$来说，x^n 是一个幂等元.

例 14.3.18 在例 14.3.14 中的有限循环单元半群 M 中，φ^3 是 ε 以外的唯一幂等元(定理 14.3.17). 对于 φ 来说，可取 $n=3$ 使 $\varphi^n=\varphi^3$ 是 M 的幂等元；对于 φ^2 来说，亦可取 $n=3$，则$(\varphi^2)^3=\varphi^6$，因$(\varphi^6)^2=\varphi^{12}=\varphi^6$，故 φ^6 也是 M 的幂等元.

14.3.3 可逆元 子半群

定义 14.3.19 设 a 为单元半群$\langle M;e\rangle$的一个元素，若存在 $x\in M$ 使$xa=e$($ax=e$)，则称 a 为**左(右)可逆元**(left, right invertible element).

若元素 $a\in M$ 既是左可逆元又是右可逆元，则称 a 为 M 的一个**可逆元**(invertible element).

例 14.3.20　(1) 单元 e 是可逆元.

(2) 一般情况下 M 的每个元素不一定都有(左、右)逆元,由例 14.2.9 的运算表可见$\langle X^X,\circ\rangle$的 ϵ 和 β 是(左、右)可逆元,但其余两个元素却不是.

定理 14.3.21　单元半群 M 的可逆元 a 有唯一的双侧逆元 a^{-1}:$a^{-1}a=aa^{-1}=e$.

每个元素都是可逆元的单元半群称为群(group),它是一种重要的代数结构(见 14.6 节).

定义 14.3.22　设$\langle A;\circ\rangle$及$\langle B;\circ\rangle$均为(单元)半群,且 $B\subseteq A$,则称$\langle B;\circ\rangle$为$\langle A;\circ\rangle$的**子(单元)半群**(sub-semigroup/sub-monoid).

注意:这个定义对于单元半群 A 来说,要求单元 e_A 也是 B 的单元,否则不能说 B 是 A 的子单元半群.这由下例可以看出:设$A=\langle\{0;1\},\cdot\rangle$,其运算由表 14.3 给出.

表 14.3

$\circ$	0	1
0	0	1
1	1	1

可证 A 是一个单元半群,其单元是 0,而且 $B_1=\langle\{1\};\circ\rangle$及 $B_2=\langle\{0\};\circ\rangle$也是单元半群,其中 B_1 的单元是 1 而 B_2 的单元是 0.将它们的单元进行比较,B_2 是 A 的子单元半群而 B_1 却不是.

定义 14.3.23　(1)设$\langle S,\circ\rangle$是半群,$T\subseteq S$,若对于 $\forall x,y\in T$ 都有 $x\cdot y\in T$,则称$\langle T,\cdot\rangle$是$\langle S,\cdot\rangle$的**子半群**.

(2) 设$\langle M,\cdot\rangle$是一个单元半群,$T\subseteq M$,

如果 1) 对于 $\forall x,y\in T$ 都有 $x\cdot y\in T$,

2) $e_M \in T$,

则称$\langle T,\cdot\rangle$是$\langle S,\cdot\rangle$的**子单元半群**(sub-monoid).

例 14.3.24 设 a 是半群 S(单元半群 M)的任意元素,则 a 的所有正整数次幂(非负整数次幂)$\{a^n\}$构成 $S(M)$的一个循环子(单元)半群(a). 特别地,对于单元半群 M 来说,若 a 是一个幂等元,则循环子单元半群(a)仅包含 a 及 e 两个元:$(a)=\{a,e\}$,由 $a^2=a$ 可以递归地推出 $a^n=a$.

(2) 在任一交换单元半群 M 中,它的所有幂等元构成一个子单元半群.

(3) 在任一单元半群 M 中,它的所有左(右)可逆元构成 M 的一个子单元半群 $L(R)$. 特别地,M 的所有可逆元构成 M 的一个子单元半群 $L\cap R$.

(4) 在模 n 同余类集 $\mathbf{Z}_n=\{C_0,C_1,\cdots,C_{n-1}\}$的关于同余类乘法"$\cdot$"构成的单元半群$\langle \mathbf{Z}_n;\cdot\rangle$中,小于 n 而且与 n 互素的正整数 k 所在的类 C_k 的集 $T=\{C_k \mid k<n,(k,n)=1\}$关于"$\cdot$"构成 $\mathbf{Z}_n$ 的一个子单元半群,可以证明这些 C_k 都是 $\mathbf{Z}_n$ 的可逆元.

下面定理对于构造子结构有重要作用.

定理 14.3.25 若 M 是单元半群,$(B_i)_{i\in I}$是由 M 的子单元半群 B_i 构成的族,I 是非空指标集,则 $B=\bigcap_{i\in I}B_i$ 仍为 M 的子单元半群.

设 A 是单元半群 M 的任一子集,则一定存在 M 的子单元半群 $B_i(A)$包含 A(例如 M 本身就是). 由定理 14.3.25 可见:若 $\{B_i(A)\mid i\in I\}$是 M 的包含 A 的子单元半群族,则$\bigcap_{i\in I}B_i(A)$也是 M 的子单元半群,而且它是 M 中包含 A 的子单元半群中的最小者.

定义 14.3.26 设 M 是一个单元半群. A 是 M 的任一子集,$B_i(A)$是 M 的包含 A 的子单元半群,则$\bigcap_{i\in I}B_i(A)$称为**由 A 生成的**

子单元半群. 而 A 则称为这个子单元半群的**生成子**(generator),用$\bigcap_{i\in I} B_i(A)=[A]$表示.

定理 14.3.27 设 M 是一个单元半群,U 是 M 的给定子集,则 M 中一切能与 U 的元素交换的元 c 所成的集 $C=\{c \mid c\in M, \forall u\in U: c\cdot u=u\cdot c\}$ 构成 M 的一个子单元半群.

定理 14.3.28 设 M 是单元半群,A,B 是 M 的两个子集,若 A 的每个元都能与 B 的每个元素交换(即 $\forall a\in A$ 及 $\forall b\in B$ 都有 $a\cdot b=b\cdot a$),则 A 所生成的子单元半群$[A]$的元素亦能与 B 的元素交换.

定理 14.3.29 设 M 是单元半群,A 是 M 的一个子集,且 A 的任二元都是可交换的(即对于 $\forall a_1, a_2\in A$,都有 $a_1\cdot a_2=a_2\cdot a_1$),则由 A 生成的最小单元半群$[A]$必是交换的.

以上关于单元半群的定义与定理稍作修改就可适用于半群. 我们知道这两个结构的差异主要在于有无单位元,因此,一个给定的半群的两个非空子半群的交可以是空集,但一个给定的单元半群的所有子单元半群均含有单元 e,它们的交集永远是非空集.

14.4 半群的同态与同构

定义 14.4.1 设$\langle S,\cdot\rangle$及$\langle S',\circ\rangle$是两个半群,$\varphi: S\to S'$是 S 到 S'的映射,若对于 $\forall x,y\in M$ 都有 $\varphi(x\cdot y)=\varphi(x)\circ\varphi(y)$,则称 φ 是 S 到 S'的一个(半群)**态射**(morphism).

定义 14.4.2 设$\langle M,\cdot\rangle$及$\langle M',\circ\rangle$是两个单元半群,$\varphi: M\to M'$是 M 到 M'的映射,若

(1) 对于所有 $x,y\in M$ 有

$$\varphi(x\cdot y)=\varphi(x)\circ\varphi(y),$$

(2) $\varphi(e_M)=e'_M$.

则称 φ 是 M 到 M' 的一个(单元半群)**态射**(morphism).

由于半群与单元半群的隶属关系以及单元半群在以后应用中的重要性,以下着重讨论单元半群的态射,这些结论稍做修改就可变成有关半群的结论.

定义 14.4.3 (1) 如果 M 到 M' 的态射 φ 是一个满射,则称 φ 是**满态射**(epimorphism)或**同态映射**(homomorphism),并称 M 与 M' **同态**,用 $M \sim M'$ 表示.

(2) 如果 M 到 M' 的态射 φ 是一个单射,则称 φ 是**单态射**(monomophism).

(3) 如果 M 到 M' 的态射 φ 是一个双射,则称 φ 是一个**同构映射**(isomorphism),并称 M 与 M' **同构**,用 $M \cong M'$ 表示.

(4) 单元半群 M 到自身的同态称为**自同态**(endomorphism).

(5) 单元半群 M 到自身的同构称为**自同构**(automorphism).

例 14.4.4 (1) $\langle \mathbf{N}; + \rangle$ 及 $\langle \mathbf{N}^+; \cdot \rangle$ 都是单元半群,作 $\mathbf{N}$ 到 $\mathbf{N}$ 的映射 $\varphi: n \mapsto 2^n$,则 φ 是一个单元半群的单态射.

(2) $\langle \mathbf{R}; + \rangle$ 到 $\langle \mathbf{R}^+; \cdot \rangle$ 间的映射 $\varphi: x \mapsto e^x$ 是一个同构映射,则有

$$\langle \mathbf{R}; + \rangle \cong \langle \mathbf{R}^+; \cdot \rangle.$$

(3) 设 $\langle \mathbf{M}; + \rangle$ 是一个交换单元半群,n 是一个给定的自然数,则映射 $\varphi: x \mapsto nx$ 是 $\langle \mathbf{M}; + \rangle$ 到自身的一个态射.

(4) $\langle \mathbf{N}; + \rangle$ 到自身的映射 $\varphi: x \mapsto x^2$ 不是单元半群态射,因为 $\varphi(n_1 + n_2) = (n_1 + n_2)^2 = n_1^2 + n_2^2 + 2n_1 n_2$,而 $\varphi(n_1) + \varphi(n_2) = n_1^2 + n_2^2$,这两个结果显然是不相等的.

定理 14.4.5 若 φ 是单元半群 M 到单元半群 M_1 的态射,ψ 是单元半群 M_1 到单元半群 M_2 的态射,则 $\psi \circ \varphi$ 是单元半群 M 到 M_2 的态射.

其示意图如图 14.1.

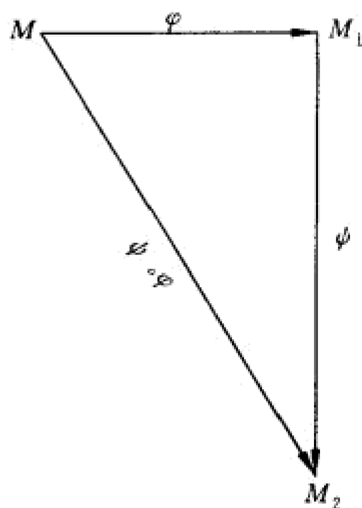


图 14.1

定理 14.4.6 设 $\langle M;\circ\rangle$ 是一个以 e 为单元的单元半群，$\langle M_1;\circ_1\rangle$ 是一个以 M_1 为基集、以 $\circ_1$ 为二元运算的代数系统，若在 M 与 M_1 间存在一个满态射 φ，则 $\langle M_1,\circ_1\rangle$ 也是一个半群. 特别地，将 $\varphi(e)$ 加入 $\langle M_1,\circ_1\rangle$ 后构成单元半群.

定理 14.4.7 设 $\varphi:M\to M_1$ 是单元半群间的同态映射，则 M 的任一子单元半群 H 在 φ 下的像 $\varphi(H)$ 是 M_1 的子单元半群.

定理 14.4.8 设 $\varphi:M\to M_1$ 是一个单元半群同态，A 是 M 的一个子集，则以 A 为生成子的子半群 $[A]$ 在 φ 下的像 $\varphi([A])$ 有性质：

$$\varphi([A])=[\varphi(A)].$$

定理 14.4.9 设 φ 与 ψ 都是单元半群 M 到单元半群 M_1 的同态映射，并且 A 是 M 的生成子：$M=[A]$，若对于任意的 $a\in A$ 都有

$$\varphi(a)=\psi(a)$$

则

$$\varphi=\psi.$$

对于同构有以下重要结果：

定理 14.4.10 若 M 与 M_1 是两个单元半群，则一个双射 $\varphi: M \to M_1$ 是一个单元半群态射当且仅当它是一个半群态射.

该定理说：对于单元半群来说，半群同构的概念是与单元半群同构的概念等价的.

定理 14.4.11 若 φ 是单元半群 M 与 M_1 间的一个同构，则逆映射 φ^{-1} 是 M_1 到 M 间的同构.

定理 14.4.12 设 φ 是单元半群 M_1 到单元半群 M_2 的同态，ϵ_{M_1}，ϵ_{M_2} 分别是 M_1，M_2 的恒等映射，若存在 M_2 到 M_1 的映射 ψ 满足

$$\psi \circ \varphi = \epsilon_{M_1}, \quad \varphi \circ \psi = \epsilon_{M_2},$$

则 φ 是 M_1 到 M_2 的同构.

定理 14.4.13 任一单元半群 $\langle M; \cdot \rangle$ 的所有态射是单元半群 $M^M = \{\varphi \mid \varphi: M \to M\}$ 的一个子单元半群.

定理 14.4.14 Cayley 定理　任何单元半群 M 都单态射于 $M^M = \{\varphi \mid \varphi: M \to M\}$ 关于映射合成构成的单元半群 $\langle M^M; \cdot \rangle$.

这个定理的意义可从下例看到：

例 14.4.15 (1) 设单元半群 M 由单元 e 及 r 个左零元 $z_1, \cdots, z_r$ 构成，由左零元意义知：

对于 $\forall i, j \in \{1, 2, \cdots, r\}$ 都有 $z_i \cdot z_j = z_i$. 作映射 $\mu: e \mapsto e_{M^M}$，$z_k \mapsto \varphi_k$，其中 $\varphi_k \in M^M$，$\varphi_k: e \mapsto z_k, z_j \mapsto z_j$，则可证 μ 是 M 到 M^M 的一个单态射，因而 M 单态射于 M^M.

(2) 在例 14.2.9 中，$X = \{0, 1\}$，X 上的 4 个变换 $\epsilon, \alpha, \beta, \gamma$ 作成单元半群 $\langle M; \circ \rangle$ 的基集 $M = \{\epsilon, \alpha, \beta, \gamma\}$. 对于任一给定的 $m \in M$，可以如下作 M 到 M 的一个映射

$$\varphi_m: x \mapsto xm \quad (x \in M).$$

显然 $\varphi_m \in M^M$. 现在 M 与 M^M 间作映射

$$\mu: m \mapsto \varphi_m,$$

则可证 μ 是一个单态射.

所以 M 单态射于 M^M.

对于循环单元半群,还有

定理 14.4.16 (1) 任一无限循环单元半群 $\mathbf{C}$ 都同构于 $\langle \mathbf{N}; + \rangle$;

(2) 任一有限循环单元半群 $\mathbf{C}=(c)$ 都同构于单元半群 $\langle M^s; \circ \rangle$,这里的 $M^s=\{0,1,\cdots,s-1\}$,乘法"·"定义如下:

对于 $$i,j\in M^s, i\cdot j=i+j-kn,$$

这里的 s 是使 $c^s=c^m$ 成立的最小正整数($m<s$),称为这个单元半群的阶(order),此时的 $n=s-m$,而 k 则是使 $k>\frac{i+j-s}{n}$ 的最小非负整数(当 $i+j<s$ 时取 $k=0$).

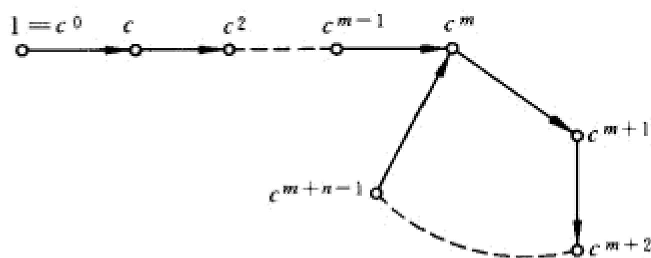


图 14.2

14.5 半群在自动机理论及形式语言中的应用

自动机理论及形式语言理论是计算机科学的基础.本节仅就它们与半群(特别是单元半群)的关系作一些介绍,我们将得到它们较深刻的数学刻画进而了解到半群在它们中的作用.

14.5.1 有限状态机器

数字计算机，都是**有限状态机器**(finite state machine)或**有限自动机**(finite state automata)，这种机器的特点如下.

(1) 计算机都是由有限个元件组成的，它们中的每一件在任一给定时刻都仅有一个**状态**，因而计算机本身有一个有限的**状态集**.

(2) 计算机是**序列的**(sequential)，它的运行同步于一个精密规定了的电子时钟信号的**时间序列**(timed sequence)，据此，每台计算机的状态在一个有序的序列中变化.

(3) 计算机都是**确定的**(deterministic)，当该机有关内部状态的信息及该机的所有输入给定后，该机的下一步动作是唯一确定的，这个动作包括该机的每个元件及输出所应采取的**下一个状态**(next state).

根据这些功能，现代计算机一般由输入装置、存储装置、算术部件、控制部件及输出装置等五部分组成. 由此给出有限状态机的定义如下：

定义 14.5.1 一有限状态自动机或有限状态机是一个五元组$\langle S,I,Z,\nu,\zeta\rangle$，其中 S 是一个**内部状态集**：$S=\{s_0,s_1,\cdots,s_n\}$；I 是**输入符号集**：$I=\{i_1,i_2,\cdots,i_l\}$；Z 是**输出符号集**：$Z=\{z_1,z_2,\cdots,z_m\}$；ν 是一个由 $S\times I$ 到 S 的**状态转换函数**(next state transition function)

$$\nu: S\times I\rightarrow S;$$

而 ζ 则是一个由 $S\times I$ 到 Z 的**输出函数**(out-put function)：

$$\zeta: S\times I\rightarrow Z.$$

有限状态机其实是三个集及两个函数构成的“五元组”(有些作者将机器在 $t=0$ 所处的“初始态”记作 S_I，即 $S_I=s_0$，并将它加

以考虑，而将有限状态机定义为六元组$\langle S,I,Z,\nu,\zeta,s_I\rangle$.).

为了简便，仅考虑具有输入符号集I及状态集S以及转换函数ν的机器，而不明显提出输出符号集及输出函数，这是因为，可以扩大状态集S使它包括任何必要的输出，只要经过适当的安排就可使一个特殊的状态产生一定的输出.

下面给出简化定义.

定义 14.5.2 一有限状态机$\langle S,I,\nu\rangle$是一个由状态集$S=\{s_1,s_2,\cdots,s_n\}$、输入符号集$I=\{i_1,i_2,\cdots,i_t\}$及一个转换函数

$$\nu: S\times I\rightarrow S$$

构成的三元组，其中转换函数用来描述每个输入值是如何改变状态的.

机器在状态s_p且被输入i_q作用时所改变到的状态记为$\nu(s_p,i_q)$.

下面是自动机的例子.

例 14.5.3 (1) 一按钮式升降机升降于1,2两个楼层之间，不运行时停于下层1. 现取该机从一层运行至另一层的时间作为基本的时间区间，而控制机则在每个区间末端改变状态. 在此机上使用三个输入值:0,1,2,因而$I=\{0,1,2\}$,其中

$$输入\ i=\begin{cases}0, & 若在前面的时间区间内未按钮;\\ 1, & 若在前面的时间区间内按下钮1;\\ 2, & 若在前面的时间区间内按下钮2\\ & 或两个钮都按下.\end{cases}$$

由于该机在未运行时停于底部，所以仅须考虑机器下降时末端的状态，故可设状态集$S=\{停,下,上—下,下—上—下\}$. 例如在“上—下”状态时，该机向上升，然后向下降. 如果未按钮或在它向上运行时按下钮1,则该机在到达层2后将回到“下”状态. 另一方面，在它到达层1时按下钮2,机器会在它到达层2时转化成

“下一上一下”状态. 此机器的转换函数 $\nu: S \times I \to S$ 可列成表 14.4.

表 14.4

次态 / 输入 / 始态	0	1	2
停	停	上一下	上一下
下	停	上一下	上一下
上一下	下	下	下一上一下
下一上一下	上一下	上一下	上一下

据此可作出机器的状态转移图 14.3,图中箭上的标号 i 表示输入,箭头两端的状态 s_p 与 s_q 表示由于输入 i 的作用使得 s_p 变成 s_q.

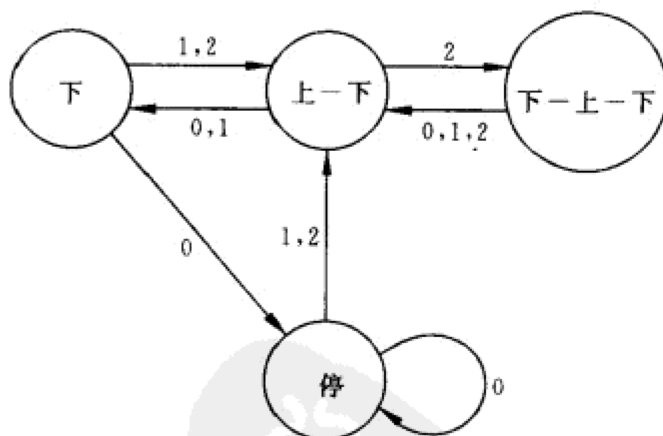


图 14.3

(2) 奇偶校验器(parity-check machine)

计算机上常需利用输入的二进制数列中含 1 的个数为奇或偶来检验编码是否有错,进而纠正错误. 为此可取状态集为 $S=\{$开始,偶,奇$\}$,输入集 $I=\{0,1\}$,其转换函数 $\nu: S \times I \to S$ 可列成表 14.5.

表　14.5

次态　输入 / 始态	0	1
开始	偶	奇
偶	偶	奇
奇	奇	偶

状态图如图 14.4

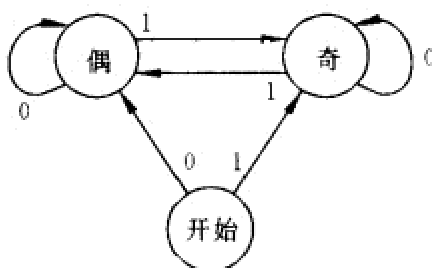


图　14.4

14.5.2　由字母表生成的自由单元半群

已知字母表Σ关于邻接运算τ分别构成半群$\langle\Sigma^+,\tau\rangle$及单元半群$\langle\Sigma^*,\tau\rangle$(见例14.2.11),设$\Sigma$是任一字母表,用$\Sigma^n$表示$\Sigma$中的由$n$个字母组成的字符串的集合.$\Sigma^n$中的字符串,称为**长度为$n$的字**(words of length n),并规定空串Λ的长度为0,则由Σ的字母组成的字符串的全体与空串Λ组成的集Σ^*可表成

$$\Sigma^* = \Sigma^0 \cup \Sigma \cup \Sigma^2 \cup \Sigma^3 \cup \cdots = \bigcup_{n=0}^{\infty} \Sigma^n.$$

定义 14.5.4　$\langle\Sigma^+;\tau\rangle$ 称为**由Σ生成的自由单元半群**(free monoid generated by Σ),也可用$\langle FM(\Sigma);\tau\rangle$表示.

在上列单元半群中,若不包括空串Λ在内,则可得到半群

$\langle \Sigma^+ ; \tau \rangle$.

定理 14.5.5 设$\langle \Sigma^* ; \tau \rangle$是由$\Sigma$生成的自由单元半群，又设$\varphi: \Sigma \to \Sigma^*$是将$\Sigma$的每个字符映射到对应的长度为1的字的函数，即$\varphi(a) = b (a \in \Sigma)$，则若$\psi$是$\Sigma$到任一单元半群$\langle M; \cdot \rangle$的基集$M$的函数：

$$\psi: \Sigma \to M,$$

则必存在唯一的一个单元半群态射

$$\sigma: \langle \Sigma^* ; \tau \rangle \to \langle M; \cdot \rangle$$

使$\sigma \circ \varphi = \psi$. 则称之为**将函数$\boldsymbol{\varphi}$通过自由单元半群$\boldsymbol{\Sigma}^*$**进行分解. 其示意图如图 14.5 .

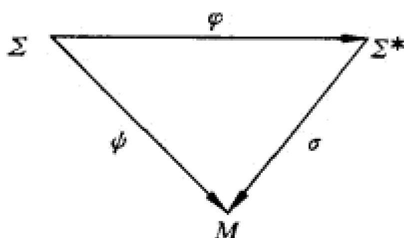


图 14.5

例 14.5.6 利用任一有限状态机$\langle S, I, \nu \rangle$的转换函数$\nu: S \times I \to S$可以定义一个新函数$\tilde{\nu}: I \to S^S$，它使每个输入值确定一个状态集$S$到其自身的函数. 这只要规定每个状态的象是所给输入产生的次状态即可，也就是说$\tilde{\nu}(i): S \to S$由$[\tilde{\nu}(i)](S) = \nu(s, i)$确定.

当输入值集合按序供给机器时，所有这些输入串作成输入值的自由单元半群$\langle \mathrm{FM}(I); \tau \rangle$的基集. 由定理 14.5.5，函数$\tilde{\nu}: I \to S^S$可以扩张成一个单元半群的态射

$$\sigma: \langle \mathrm{FM}(I); \tau \rangle \to \langle S^S; \circ \rangle.$$

这里的$\sigma(i_1 i_2 \cdots i_r) = \tilde{\nu}(i_1) \circ \tilde{\nu}(i_2) \circ \cdots \circ \tilde{\nu}(i_r)$.

(注意,这里的输入值应按由右至左的方向供给机器,即先供给 i_r,然后至 i_{r-1} 等等).

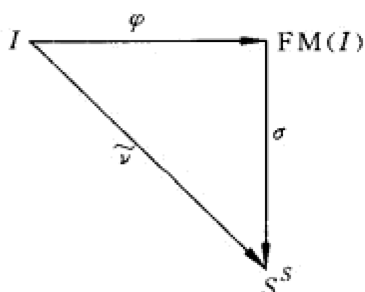


图 14.6

现在进一步以奇偶校验器为例加以解释:

此机器用于检验串中含 1 的个数的奇偶性,其状态集 $S=\{$开始,偶,奇$\}$,定理中的两个函数是

$$\tilde{\nu}:\{0,1\}\to S^S \quad 及\ \sigma:\mathrm{FM}(\{0,1\})\to S^S.$$

态射 σ 被定义为

$$\sigma(串)=\begin{cases}\tilde{\nu}(0), & 当串含有偶数个 1 时;\\ \tilde{\nu}(1), & 当串含有奇数个 1 时;\\ S 上的恒等函数, & 当串是空串时.\end{cases}$$

14.5.3 商单元半群及机器的单元半群

考察有限状态机的一个重要构造问题. 在例 14.5.6 中的奇偶校验器中,不同的输入串对于该机可以有相同的效应(effect),例如串 0101101,0000,11 及 0 中所含 1 的个数都是偶数,所以它们对应的函数值都相等:

$$\sigma(0101101)=\sigma(0000)=\sigma(11)=\sigma(0).$$

一般地,设 $\langle S,I,\nu\rangle$ 是一个具有 n 个状态的机器,则它至多只

能有$|S^S|=n^n$个不同的效应. 但是在 FM(I)中却有无穷多个串，因此必有很多不同的串有相同的效应. 在自由单元半群 FM(I)的串间定义关系 R 如下：

$\alpha R\beta \Leftrightarrow \alpha$ 与 β 对于机器有相同的效应.

可证明 R 是 FM(I)上的一个等价关系. 商集 FM(I)/R,它的每个块是由有相同效应的所有串组成的,用$[\alpha]$表示与 α 有相同效应的串组成的块：

$$[\alpha]=\{\xi \mid \xi \in \mathrm{FM}(I), \xi R\alpha\}.$$

则

$$\mathrm{FM}(I)/R=\{[\alpha],[\beta],\cdots\}.$$

在商集 FM(I)/R 中还可利用 FM(I)中串的邻接运算 τ 规定块的代数运算 τ：

$$[\alpha]\tau[\beta]=[\alpha\,\tau\,\beta].$$

至此可得如下定理.

定理 14.5.7 $\langle \mathrm{FM}(I)/R;\tau\rangle$构成一个单元半群.

定义 14.5.8 $\langle \mathrm{FM}(I)/R;\tau\rangle$称为**机器**$\langle S,I,\nu\rangle$**的单元半群**.

例 14.5.9 (1) 机器$\langle S,I,\nu\rangle$的 $S=\{s_0,s_1\}$, $I=\{0,1\}$. 输入串的效应由函数 $\sigma(0),\sigma(1):S\to S$ 给出,如表 14.6.

表 14.6

初态	次态	
	$\sigma(0)$	$\sigma(1)$
s_0	s_0	s_1
s_1	s_0	s_0

因为 σ 是态射,故可利用

$$\sigma(i \circ j) = \sigma(i) \circ \sigma(j)$$

计算出长度为 2 的字符串 00,01,10,11 的 σ 值如表 14.7：

表 14.7

初　态	末　态			
	$\sigma(00)$	$\sigma(01)$	$\sigma(10)$	$\sigma(11)$
s_0	s_0	s_0	s_1	s_0
s_1	s_0	s_0	s_1	s_1

因为 $|S^S| = 2^2 = 4$，此机器所能产生的不同效应的个数不能超过 4. 由表 14.6 看到 $\sigma(00) = \sigma(01) = \sigma(0)$，因而此机器单元半群中的块[00]、[01]及[0]相等. 故整个单元半群由 4 个共轭块[0]，[1]，[10]及[11]组成，其运算表如表 14.8 及状态图如图 14.7，由表 14.8 可见它的单元是[11]，它有两个左零元[0]及[10]，但却没有右零元.

表 14.3

$\circ$	[0]	[1]	[10]	[11]
[0]	[0]	[0]	[0]	[0]
[1]	[10]	[11]	[0]	[1]
[10]	[10]	[10]	[10]	[10]
[11]	[0]	[1]	[10]	[11]

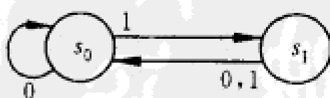


图 14.7

(2) 在奇偶校验器⟨{开始,偶,奇},{0,1},ν⟩中(例 14.5.3(2),例 14.5.6),我们早已知道有偶数多个 1 的输入串与 0 有相同的效应,而有奇数多个 1 的串则与 1 有相同的效应.据此可作出状态转换表 14.9.

表 14.9

初　　态	次　　态		
	$\sigma(\Lambda)$	$\sigma(0)$	$\sigma(1)$
开始	开始	偶	奇
偶	偶	偶	奇
奇	奇	奇	偶

由于它们所产生的效应各不相同,故此机器的单元半群由三个类$[\Lambda]$,$[0]$及$[1]$组成,其运算表如表 14.10,空串类$[\Lambda]$显然是它的单元.

表 14.10

$\circ$	$[\Lambda]$	$[0]$	$[1]$
$[\Lambda]$	$[\Lambda]$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[1]$	$[0]$

14.6 群的定义及例子

群是一种重要的代数结构,下面给出群的定义.

定义 14.6.1 设$\langle G;\cdot\rangle$是单元半群,若它的每个元素都是可逆的,则称 G 是**群**(group).

因为 G 的每个元素 a 都是可逆的. 所以它的逆元 a^{-1} 存在. 群还有另外的定义.

定义 14.6.2 设 $\langle G;\cdot\rangle$ 是一个单元半群，如果它满足下列条件：

(1) 结合律：对于 $\forall x,y,z\in G$ 都有

$$x\cdot(y\cdot z)=(x\cdot y)\cdot z;$$

(2) 存在单元 e，对于 $\forall x\in G$ 都有

$$e\cdot x=x\cdot e=x;$$

(3) 对于 $\forall x\in G$，存在逆元 $x^{-1}\in G$ 使

$$x\cdot x^{-1}=x^{-1}\cdot x=e.$$

则称 G 是**群**. 群的定义中的条件还可以减弱.

定义 14.6.3 代数系统 $\langle G;\cdot\rangle$，如果它满足下列条件：

(1) 结合律(同定义 14.6.2)；

(2) 存在一个左(右)单元 $e_l(e_r)$，对于 $\forall x\in G$ 都有 $e_l\cdot x=x(x\cdot e_r=x)$；

(3) 对 $\forall x\in G$ 都有一个左(右)逆元 $x_l^{-1}(x_r^{-1})$ 使

$$x_l^{-1}\cdot x=e_l\quad(x\cdot x_r^{-1}=e_r).$$

则称 G 是**群**.

可以证明定义 14.6.3 中的左单元同时也是 G 的右单元，元素 x 的左逆元同时也是它的右逆元.

为了突出单元及逆元在群中的地位，有时也将求群的单元 e 与求元素 a 的逆元 a^{-1} 看作两种运算，并分别称为**零元运算**(nullary operation)及**一元运算**(unary operation). 并分别用 e 及 $^{-1}$ 表示，这样在一个群 $\langle G;\cdot\rangle$ 中就有了三种运算，即零元运算 e、一元运算 $^{-1}$ 及群中原来的二元运算. 具体写出是 $\langle G;e,{}^{-1},\cdot\rangle$.

定理 14.6.4 (1) 设 G 是一个群，则它的方程 $ax=b$ 及 $ya=b(a,b\in G)$ 必有解，它们的解分别是 $x=a^{-1}b$ 及 $y=ba^{-1}$；

(2) 如果半群$\langle G;\cdot\rangle$的方程 $ax=b$ 及 $ya=b$ 在 G 里都有解，那么这个半群构成一个群.由此可得群的另一个等价定义：

定义 14.6.5 设$\langle G;\cdot\rangle$是半群.若$\forall a,b\in G$,方程 $ax=b$ 及 $ya=b$ 在 G 中都有解,则称它为**群**.

定义 14.6.6 若群$\langle G;\cdot\rangle$的乘法是可交换的.则称为 **Abel 群**(Abel group)或**交换群**(commutative group).

定义 14.6.7 若群 G 的元素个数是有限的,则称它为**有限群**(finite group),否则称为**无限群**(infinite group).

一个半群是否是群,一般要检验它是否有单元及它的每个元素是否有逆元.但是对有限半群检验工作可以简化,因为有以下定理.

定理 14.6.8 若在一个有限半群$\langle G;\cdot\rangle$中以下两个消去律成立：

若 $ax=ax'$,则 $x=x'$;

若 $ya=y'a$,则 $y=y'$,

则$\langle G;\cdot\rangle$是一个群.

例 14.6.9 (1) 非零有理数集 $\mathbf{Q}^*$ 关于数的乘法"·"构成一个交换群$\langle\mathbf{Q}^*;\cdot\rangle$,其单元是有理数 1,每个 $q\in\mathbf{Q}^*$ 的逆元是 q 的倒数 $1/q$.

(2) 非零实数集 $\mathbf{R}^*$,非零复数集 $\mathbf{C}^*=\{x+y\mathrm{i}\mid x,y\in\mathbf{R},\ x,y$ 不同时为零$\}$关于数的乘法各构成一个交换群$\langle\mathbf{R}^*;\cdot\rangle$及$\langle\mathbf{C}^*;\cdot\rangle$.

(3) 非零整数集 $\mathbf{Z}^*$ 关于数的乘法"·"不构成群.因为除± 1外每个非零整数的倒数不在其内.

(4) 整数集 $\mathbf{Z}$ 关于数的加法"+"构成一个交换群$\langle\mathbf{Z};+\rangle$,称之为整数加群.

(5) 模为 1 的复数集 U、数 1 的 n 次单位根的集 U_n 关于复数乘法分别构成交换群$\langle U;\cdot\rangle$及$\langle U_n;\cdot\rangle$.

例 14.6.10 在例 14.2.9 中，$\langle X^X;\circ\rangle$构成一个单元半群. 现取 X^X 中的所有 1-1 变换(即 X 到 X 的一切双映射)的集 G. 它关于变换的复合构成一个群$\langle G;\cdot\rangle$，称之为 X 上的**变换群**(transformation group). 其单元是恒等变换 ϵ: $x\mapsto x$. 变换 τ: $x\mapsto X'$的逆元是 τ 的逆变换 τ^{-1}: $X'\mapsto x$. 特别，若 X 是由 n 个元素构成的有限集，则它的变换群 S_n 称为 ***n* 次对称群**(symmetric group). 这个群共有 $n!$ 个元素.

例 14.6.11 平面上所有绕坐标原点作 θ 角旋转的 r_θ 的集 $G=\{r_\theta\,|\,-\infty<\theta<+\infty\}$. 关于旋转的复合"$\circ$": $r_{\theta_1}\circ r_{\theta_2}=r_{\theta_1+\theta_2}$ 构成一个交换群$\langle G;\circ\rangle$，它的单元是恒等旋转 r_0. r_θ 的逆元是 $r_{-\theta}$.

例 14.6.12 平面上一切从原点出发的向量的集合 $V=\{(a,b)\,|\,a,b\in\mathbf{R}\}$关于向量加法"+"构成一个交换群，其单元是零向量 $\mathbf{0}=(0,0)$、向量 $\boldsymbol{v}=(a,b)$的逆元是$-\boldsymbol{v}=(-a,-b)$.

14.7 群的基本性质

群是一种特殊的单元半群. 因此具有单元半群的一切性质. 由于它的每个元素都有逆元，所以它有更丰富的内容.

定理 14.7.1 群的单元 e 是存在且唯一的.

定理 14.7.2 设$\langle G;\cdot\rangle$是一个群，$a\in G$，则它的逆元 a^{-1} 是存在且唯一的.

定理 14.7.3 设$\langle G;\cdot\rangle$是群，$a,b\in G$，则:

(1) $(a^{-1})^{-1}=a$;

(2) $(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}$.

定理 14.7.3 中的结论(2)还可以推广到有限多个元素乘积求逆元.

我们使用 a^{-1}代表 a 的逆元，主要是为了推广元素 a 的幂的

概念.在定义 14.3.2 中已定义了元素 a 的零次幂,如果规定 a 的负整数次幂为:

(1) a^{-1} 代表 a 的逆元;

(2) 设 n 是一个负整数 $n=-m$,规定

$$a^n = a^{-m} = (a^{-1})^m.$$

则可以将定理 14.3.3~定理 14.3.6 的幂的运算法则推广到全体整数指数幂中去.

定理 14.7.4 在群 G 中,对于 $\forall a \in G$ 及 $\forall m, n \in \mathbf{Z}$,有 $a^m \cdot a^n = a^{m+n}$.

定理 14.7.5 在群 G 中对于 $\forall a \in G$ 及 $\forall m, n \in \mathbf{Z}$,有 $(a^n)^m = a^{n \cdot m}$.

定理 14.7.6 设 G 是一个交换群,对于 $\forall a, b \in G$, $\forall m \in \mathbf{Z}$,有 $(a \cdot b)^m = a^m \cdot b^m$.

定理 14.7.7 群的乘法满足:

(1) 左消去律:若 $ax = ax'$,则 $x = x'$;

(2) 右消去律:若 $ya = y'a$,则 $y = y'$.

注意:满足两个消去律的半群未必能成群,例如非零整数集 $\mathbf{Z}^*$ 关于乘法构成一个单元半群,它满足两个消去律,但却不是群(例 14.6.9),仅当它是有限半群时方能成群(见定理 14.6.8).

定理 14.7.8 在一个群中,方程 $ax = b$ 及 $ya = b$ 各有一个唯一解 $x = a^{-1}b$ 及 $y = ba^{-1}$.

下面介绍群中元素的阶及群的阶等概念.

定义 14.7.9 设 $\langle G; \cdot \rangle$ 是群,$a \in G$,则使

$$a^m = e$$

成立的最小正整数 m 叫做元素 a 的**阶** (order).若这样的正整数不存在,则称 a 的**阶是无限的**.

定义 14.7.10 设 $\langle G; \cdot \rangle$ 是一个有限群,则 G 中元素个数

$|G|$称为群 G 的阶.

例 14.7.11 U_3 由 1 的三个立方根 $\omega_{1,2}=\dfrac{-1\pm\sqrt{3}\,\mathrm{i}}{2}$ 及 $\omega_0=1$ 组成. 由例 14.6.9,$\langle U_3;\cdot\rangle$是一个有限集,它的阶是 3,它的元素 $\omega_0=1$ 的阶是 1,ω_1 及 ω_2 的阶都是 3.

定理 14.7.12 有限群中每个元素的阶都是有限的,且它们的阶不大于群 G 的阶$|G|$.

定理 14.7.13 群中的元素 a 与它的逆元 a^{-1}有相同的阶.

定理 14.7.14 设群 G 的元素 a 的阶为 m,则 $a^k=e$ 的充要条件是:$k=tm(t\in\mathbf{Z}^*)$(即 k 可被 m 整除).

定理 14.7.15 在一个有限群中,阶大于 2 的元素的个数一定是偶数.

定理 14.7.16 若有限群 G 的阶是偶数,则 G 中阶等于 2 的元素的个数一定是奇数.

14.8 子群

客观上存在很多子群,如例 14.6.9 的$\langle\mathbf{Q}^*;\cdot\rangle$是$\langle\mathbf{R}^*;\circ\rangle$的子群. 而$\langle\mathbf{R}^*;\cdot\rangle$又是$\langle\mathbf{C}^*;\cdot\rangle$的子群等等. 可以通过子群及其所构成的新结构来探索原群的构造.

定义 14.8.1 设$\langle G;\cdot\rangle$是群,H 是 G 的非空子集. 若$\langle H;\cdot\rangle$是群,则称它为$\langle G;\cdot\rangle$的**子群**(subgroup),有时简称 H 是 G 的子群.

例 14.8.2 $\langle\mathbf{Q}^*;\cdot\rangle$是$\langle\mathbf{R}^*;\cdot\rangle$的子群. $\langle\mathbf{R}^*;\cdot\rangle$是$\langle\mathbf{C};\cdot\rangle$的子群. 其实任何群 G 都有子群,因为 G 就是 G 本身的子群,且由它的单元 e 构成的集$\{e\}$也是 G 的子群. 这两个子群称为**平凡子群**(trivial subgroup). 其他的子群(如果存在的话)称为 G

的**真子群**(proper subgroup).

下面是检验子集 H 构成 G 的子群的方法.

定理 14.8.3 设 $\langle G;\cdot\rangle$ 是群，$H\subseteq G$ 是一个非空集，若它满足以下条件，则 $\langle H;\cdot\rangle$ 是 $\langle G;\cdot\rangle$ 的子群：

(1) 运算"·"在 H 内是封闭的，即对于 $\forall a,b\in H, a\cdot b\in H$；

(2) 对于 $\forall a\in H$，其逆元 $a^{-1}\in H$.

此定理的条件还可以简化如下.

定理 14.8.4 设 $\langle G;\cdot\rangle$ 是群，$H\subseteq G$ 是一个非空集，若它满足以下条件，则 $\langle H;\cdot\rangle$ 是 $\langle G;\cdot\rangle$ 的子群：

若对于 $\forall a,b\in H$，则 $a\cdot b^{-1}\in H$.

若子集 H 是有限的，则可以进一步简化如下.

定理 14.8.5 设 $\langle G;\cdot\rangle$ 是群，$H\subseteq G$ 是一个有限集. 则 $\langle H;\cdot\rangle$ 是 $\langle G;\cdot\rangle$ 的有限子群的充要条件是：若 $a,b\in H$，则 $a\cdot b\in H$.

最后给出一个构造群 G 的子群的方法.

定理 14.8.6 设 $\langle G;\cdot\rangle$ 是群，S 是 G 的非空子集. 令 $H=\{S$ 的元素的各种整数次幂之积$\}$，则 H 是 G 中包含 S 的最小子群.

定义 14.8.7 定理 14.8.6 中构成的最小子群 H 称为 S 生成的子群，集 S 称为子群 H 的**生成子(集)**(generator).

14.9 特殊群

本节介绍三种最重要的具体群：变换群、置换群及循环群. 可以看到：任何群都可在变换群中找到一个"模型"，任何有限群都可在置换群中找到一个"模型". 至于循环群则是近世代数所研究问题的缩影，因为在循环群里三个主要问题都已得到完满的解决.

14.9.1 变换群

在例 14.6.10 中已介绍过这种群，现给出它的定义.

定理 14.9.1 设 X 是集，X 到 X 的双射称为 X 的**一一变换**. 由 X 的所有一一变换构成的集 $T(X)$ 关于复合运算"$\circ$"构成一个群 $\langle T(X);\circ\rangle$.

注意：在例 14.2.9 中我们已看到 X^X 关于复合运算"$\circ$"构成一个单元半群，但它不能构成群，可以证明，X^X 的子集 A 构成群的必要条件是 A 仅由 X 上的一一变换组成.

定义 14.9.2 $\langle T(X);\cdot\rangle$ 以及它的子群都称为集 X 上的**变换群**(transformation group).

例 14.9.3 (1) 设 $X=\{1,2,3\}$，则 X 上的一一变换有以下 6 个：

π_1：$1\mapsto 1$，$2\mapsto 2$，$3\mapsto 3$　　　π_2：$1\mapsto 1$，$2\mapsto 3$，$3\mapsto 2$，

π_3：$1\mapsto 2$，$2\mapsto 1$，$3\mapsto 3$　　　π_4：$1\mapsto 2$，$2\mapsto 3$，$3\mapsto 1$，

π_5：$1\mapsto 3$，$2\mapsto 1$，$3\mapsto 2$　　　π_6：$1\mapsto 3$，$2\mapsto 2$，$3\mapsto 1$.

此时 $T(X)=\{\pi_1,\pi_2,\pi_3,\pi_4,\pi_5,\pi_6\}$.

群 $\langle T(X);\cdot\rangle$ 是 X 上的一个变换群.

可以验证，$T_1=\{\pi_1,\pi_2\}$ 及 $T_2=\{\pi_1,\pi_3\}$ 都是 $\langle T(X);\cdot\rangle$ 的子群. 因此 $\langle T_1;\circ\rangle$ 及 $\langle T_2;\circ\rangle$ 也是 X 上的变换群.

(2) 设 X 是平面上所有点的集合. 将平面的一个绕原点作 θ

角的旋转 r_θ 看成 X 的一个一一变换. 作 $G=\{r_\theta \mid -\infty<\theta<+\infty\}$. 由定义 14.6.11 知, $\langle G;\circ\rangle$ 构成一个群. 因而 G 是平面上的一个变换群.

定理 14.9.4 Cayley 定理　任何一个群 $\langle G;\circ\rangle$ 都与一个变换群同构.

两个代数结构如果是同构的,则把它们看成是相同的(对于它们的运算来说),只是它们使用的符号不同. 这方面的例子已有例 14.4.15. 令人惊讶的是,本定理却断言任何抽象复杂的群都能找到一个具体的变换群作为它的"模型",可见变换群在群的理论中的重要地位. 通过以下的例子可看到该定理的作用及其证明梗概.

例 14.9.5 (1) 设群 $G=\{a,b,c,\cdots\}$,其代数运算是"$\circ$". 今利用 G 的元素作集 G 的一一变换 τ_x 如下:

$$\tau_x:\ g\mapsto g\circ x \quad (\forall g\in G)$$

作 $T(G)=\{\tau_a,\tau_b,\tau_c,\cdots\}$,今在 G 与 $T(G)$ 间作映射

$$\varphi:\ x\mapsto\tau_x.$$

则可证 φ 是 G 与 $T(G)$ 间的同构映射,即 $G\cong T(G)$.

(2) 在三次单位根所作成的群 $U_3=\{\omega_0,\omega_1,\omega_2\}$ 中(例 14.7.11), $\omega_1=\dfrac{-1+\sqrt{3}\mathrm{i}}{2}$, $\omega_2=\dfrac{-1-\sqrt{3}\mathrm{i}}{2}=\omega_1^2$, $\omega_0=\omega_1^3=1$. 故 $U_3=\{\omega_1^3=1,\omega_1,\omega_1^2\}$,其运算(乘法)如表 14.11.

作 U_3 上的一一变换 τ_x 如下: $\tau_x:\ g\mapsto g\cdot x \quad (\forall g\in U_3)$,

则 $\tau_1:\ 1\mapsto 1 \quad (1\in U_3)$

$\omega_1\mapsto\omega_1$

$\omega_1^2\mapsto\omega_1^2$,

$\tau_{\omega_1}:\ 1\mapsto\omega_1 \quad (\omega_1\in U_3)$

$\omega_1\mapsto\omega_1^2$

$\omega_1^2\mapsto\omega_1^3=1$,

$\tau_{\omega_1^2}: 1 \mapsto \omega_1^2 \quad (\omega_1^2 \in U_3)$

$\omega_1 \mapsto \omega_1^3 = 1$

$\omega_1^2 \mapsto \omega_1$.　　所以 $T(U_3)=\{\tau_1, \tau_{\omega_1}, \tau_{\omega_1^2}\}$

其运算如表 14.12.

表 14.11

$\cdot$	1	ω_1	ω_1^2
1	1	ω_1	ω_1^2
ω_1	ω_1	ω_1^2	1
ω_1^2	ω_1^2	1	ω_1

表 14.12

$\circ$	τ_1	τ_{ω_1}	$\tau_{\omega_1^2}$
τ_1	τ_1	τ_{ω_1}	$\tau_{\omega_1^2}$
τ_{ω_1}	τ_{ω_1}	$\tau_{\omega_1^2}$	τ_1
$\tau_{\omega_1^2}$	$\tau_{\omega_1^2}$	τ_1	τ_{ω_1}

在 U_3 与 $T(U_3)$ 间作映射

$$\varphi: X \mapsto \tau_X,$$

则可证 φ 是一个同构映射.(由这两个运算表有相同的构造已可见到).

所以 $\langle U_3; \cdot \rangle \cong \langle T(U_3); \circ \rangle$.

14.9.2 置换群

置换群是变换群的特例,它是基集 X 为有限集时的变换群,因此,它具有变换群的一切性质,又因它的有限性,在表示方面有比较简单的形式.它在代数学中,特别是在方程根式解的问题中特别重要.

定义 14.9.6 有限集 A 上的一个一一变换叫做一个**置换**(permutation).

定义 14.9.7 一个有限集上的若干个置换构成的群称为**置换群**(permutation group).

定义 14.9.8 包含 n 个元素的集上的全体置换构成的群称为 n **次对称群**(symmetric group).用 S_n 表示.

例 14.9.9 三元集 $X=\{1,2,3\}$ 上的置换 $\pi_1, \pi_2, \pi_3, \pi_4, \pi_5$,

π_6，这 6 个置换的全体构成一个三次对称群 S_3（见例 14.9.3）；它及它的子群如$\{\pi_1,\pi_2\}$，$\{\pi_1,\pi_3\}$等都是置换群.

下面讨论置换的表示. 一般有三种方法：

表示法 14.9.10 列表法 设有限集 $X=\{a_1,a_2,\cdots,a_n\}$，则它上面的置换 π 可表成

$$\pi:\ a_i \mapsto a_{k_i} \quad (i=1,2,\cdots,n).$$

为了简便，可省去字母 a 而直接用它们的下标来表示. 因而可分别表示成 $X=\{1,2,\cdots,n\}$. 及

$$\pi:\ i \mapsto k_i \quad (i=1,2,\cdots,n).$$

通常把它们写成上下对应的表：

$$\pi=\begin{pmatrix}1 & 2 & \cdots & i & \cdots & n\\ k_1 & k_2 & \cdots & k_i & \cdots & k_n\end{pmatrix}.$$

表中上行记下标 i，而在 i 的下方记下它的像 k_i. 至于上行各下标数是否依自然顺序排列是无关紧要的.

两个置换 π_1,π_2 的“乘积”可定义如下：

(1) 从 π_1 中的第 1 行的“1”开始，找到它的像 $k_1=\pi(1)$，然后在 π_2 中第 1 行的 k_1 下方找到 k_1 在 π_2 下的像 $k_1'=\pi_2(k_1)$，此 k_1' 就是置换 $\pi_1\cdot\pi_2$ 中数 1 的像 $k_1'=\pi_1\cdot\pi_2(1)$.

(2) 再从 π_1 中的第 1 行的“2”下找到它的像 $k_2=\pi_1(2)$，然后在 π_2 中第 1 行的 k_2 下方找到它在 π_2 下的像 $k_2'=\pi_2(k_2)$，该 k_2' 就是置换 $\pi_1\cdot\pi_2$ 中数 2 的像 $k_2'=\pi_1\cdot\pi_2(2)$. 以下仿此.

以例 14.9.3 的三次对称群 $S_3=\{\pi_1,\cdots,\pi_6\}$为例，各置换可表成：

$$\pi_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix},\quad \pi_2=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix},$$

$$\pi_3=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},\quad \pi_4=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},$$

$$\pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

至于这些置换的乘积(如 $\pi_3 \cdot \pi_4$ 及 $\pi_4 \cdot \pi_3$),则可分别计算如下:

$$\pi_3 \cdot \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\pi_4 \cdot \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

由此可见,$\pi_3 \cdot \pi_4 \neq \pi_4 \cdot \pi_3$,故 S_3 是一个非交换群,而且它是阶数最小的非交换群.可以证明,所有阶数小于 6 的群都是可交换的.

表示法 14.9.11 表成循环置换的积

首先介绍一个定义:

定义 14.9.12 设 $a_{i_1}, \cdots, a_{i_k}$ 两两不同,S_n 中的一个把 a_{i_1} 变到 a_{i_2},a_{i_2} 变到 a_{i_3},$\cdots$,a_{i_k} 变到 a_{i_1},而其余的元素不变的置换,叫做一个 ***k*-循环置换**(*k*-cycle).用$(i_1 i_2 \cdots i_k)$,$(i_2 i_3 \cdots i_k i_1)$,$\cdots$或$(i_k i_1 \cdots i_{k-1})$表示.

例 14.9.13 把下列置换表示成循环置换,或循环置换的积.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5) = (2\ 3\ 4\ 5\ 1) = (3\ 4\ 5\ 1\ 2)$$
$$= (4\ 5\ 1\ 2\ 3) = (5\ 1\ 2\ 3\ 4).$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1\ 2\ 3)(4\ 5) = (2\ 3\ 1)(4\ 5)$$
$$= (3\ 1\ 2)(5\ 4).$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2).$$

注意:在置换中元素不变的部分,可以在循环置换中出现,也可以不出现.例如“恒等置换”$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$根据定义 14.9.12

可以表示成(1)(因为在这个置换中元素 1 变成 1,而其余的元素不变),也可以变成(2)(因为在这个置换中元素 2 变成 2,而其余的元素不变),因此有 $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}=(1)=(2)=(3)=(4)=(5)$. 然而由于这种仅含一个元素的循环置换只表示恒等置换,其作用与单位元素相同,所以常常可以省去!

例如

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 4 & 5\end{pmatrix}=(1\ 2\ 3)=(2\ 3\ 1)=(3\ 1\ 2)$$
$$=(1\ 2\ 3)(4)=(2\ 3\ 1)(5)=\cdots$$

定理 14.9.14 任意的 n 元置换 π 均可表示成一个循环置换或若干个没有共同数字的循环置换的乘积.

例 14.9.15 例 14.9.13 中的三个置换均已表成循环置换.

S_4 的 $\pi=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$ 虽不是一个循环置换,但可写成两个循环置换的乘积.

$$\pi=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}=(1\ 2)(3\ 4).$$

同理 S_5 的 $\pi=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 1 & 5 & 2 & 3\end{pmatrix}=(1\ 4\ 2)(3\ 5)$.

例 14.9.3 中的 6 个置换可表成以下的循环置换:

$\pi_1=(1)$, $\pi_2=(2\ 3)$, $\pi_3=(1\ 2)$, $\pi_4=(1\ 2\ 3)$,

$\pi_5=(1\ 3\ 2)$, $\pi_6=(1\ 3)$.

表示法 14.9.16 表成对换的乘积 S_n 中的(1 2), (1 3),…, (1 n)称为 2-**循环置换**或**对换**(transposition).

一般,设循环置换 $\pi=(i_1 i_2 \cdots i_k)$,则 $\pi=(i_1 i_2 \cdots i_k)=(i_1 i_2)(i_1 i_3)\cdots(i_1 i_k)$,根据定理 14.9.14 即知,$S_n$ 的任一置换均可

表成若干个 k-循环置换，从而表成若干个对换的乘积.

定理 14.9.17 n 次对称群的阶是 $n!$

定理 14.9.18 Cayley 定理　每个有限群都与一个置换群同构.

例 14.9.19 例 14.9.5 的 $U_3=\{1,\omega_1,\omega_1^2\}$ 是一个群，为了表示它上面的置换，用数码 1，2，3 分别表示 U_3 的 $1,\omega_1,\omega_1^2$，则得 $\pi_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=(1)$，$\pi_{\omega_1}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(1\ 2\ 3)$，$\pi_{\omega_1^2}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(1\ 3\ 2)$，从而得置换群 $T(U_3)=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$，作 U_3 到 $T(U_3)$ 间的映射

$$\begin{aligned}\varphi:1&\mapsto\pi_1\ =(1),\\ \omega&\mapsto\pi_{\omega_1}\ =(1\ 2\ 3),\\ \omega^2&\mapsto\pi_{\omega_1^2}=(1\ 3\ 2).\end{aligned}$$

可证明 φ 是 U_3 与 $T(U_3)$ 间的同构映射.

14.9.3 循环群

定义 14.9.20 设 $\langle G;\circ\rangle$ 是一个群，若它的每个元素 g 都是 G 的某个元素 a 的整数次幂：$g=a^m(m\in Z)$，则称该群为由 a 生成的**循环群**(cyclic group). 用 $G=\langle a\rangle$ 表示，并称 a 是 G 的一个**生成元**.

例 14.9.21 (1) 如果把整数加群 $\langle \mathbf{Z};+\rangle$(见例 14.6.9)的代数运算不用“+”而用“∘”表示，这个群的元素就都是 1 的整数次“幂”，因若设 m 是任一正整数，则

$$m=\underbrace{1+1+\cdots+1}_{m个}=\underbrace{1\circ 1\circ\cdots\circ 1}_{m个}=1^m,$$

$$-m=\underbrace{(-1)+(-1)+\cdots+(-1)}_{m个}=\underbrace{(-1)\circ(-1)\circ\cdots\circ(-1)}_{m个}$$

$$=(1^{-1})\circ(1^{-1})\circ\cdots\circ(1^{-1})$$

$$=1^{-m}.$$

这样 G 的非零整数都是 1 的整数次“幂”. 由于 0 是 G 的单元，依定义：$0=1^0$. 所以 G 中每个元素都是它的元素 1 的整数次“幂”，所以 $G=\langle \mathbf{Z};+\rangle$ 是一个循环群. 它的生成元是 1，即 $G=\langle 1\rangle$.

(2) 在模 n 的同余类集 $\mathbf{Z}/(n)=\{[0],[1],[2],\cdots,[n-1]\}$ 中规定代数运算（仍用数的加法符号＋表示）如下：

$$[a]+[b]=[a+b],$$

则 $\langle \mathbf{Z}/(n);+\rangle$ 也是一个交换群，称它为模 n 的同余类加群. 可以证明它的每个元素 $[k]$ $(0\leqslant k\leqslant n-1)$ 都可以写成 $[1]$ 的某一整数次幂：

$$[k]=[1]^k,$$

所以 $\mathbf{Z}/(n)$ 是一个由 $[1]$ 生成的循环群，$\mathbf{Z}/(n)=\langle [1]\rangle$.

定理 14.9.22 设 $G=\langle a\rangle$ 是一个由 a 生成的循环群，则它的构造完全由 a 的阶来决定：

(1) 若 a 的阶是无限的，则 $G\cong\langle \mathbf{Z};+\rangle$；

(2) 若 a 的阶是有限整数 n，则 $G\cong\langle \mathbf{Z}/(n);+\rangle$.

例 14.9.21 及定理 14.9.22 圆满地回答了近世代数学对于代数结构提出的三大问题：就存在问题说，通过例 14.9.21 我们已有两个循环群（整数加群及模 n 的同余类加群），因此循环群确实存在. 本定理告诉我们，抽象地看，循环群也仅限于这两种，循环群的构造完全决定于它的生成元的阶：如果它的阶是无限的，那么它就是整数加群；如果它的阶 n 是有限整数，那么它就是模 n 的同余类加群，而这两个循环群的构造是大家所熟知的. 因此循环群的数量问题和构造问题也同时得到了完满的答复.

14.10 群的分解

本节将利用群的子群对群进行分类，通过分类来研究原群的性质；如果利用的子群是一些特殊的子群（正规子群），则这些类还可以构成一个与原群有密切关系的新群（商群，或称因子群）作为研究原群性质的工具. 其实这种方法早在前人研究整数的整除性时就已经使用过了. 例如模 n 同余类加群 $\langle \mathbf{Z}/(n);+\rangle$ 就是在整数加群 $\langle \mathbf{Z};+\rangle$ 中利用子群 (n) 构造出来的商群.

14.10.1 群的陪集分解

已知集的划分与集合元素的等价关系间存在着密切的联系. 为了对群 G 进行划分，必须在它的元素间找出一个等价关系. 通常若 H 是群 G 的一个子群，则利用 H 可建立的群 G 的元素间的关系～：

$$\forall a,b\in G,\ a\sim b \Leftrightarrow ab^{-1}\in H,$$

它是一个等价关系.

定义 14.10.1 由上述等价关系"～"所决定的集叫做子群 H 的**右陪集**(right coset). 包含元素 a 的右陪集称为 a 所在的右陪集，记作 Ha.

定理 14.10.2 设 H 是群 G 的子群，$a\in G$，则 a 所在的右陪集 Ha 由一切形如 $ha\,(h\in H)$ 的元素构成：

$$Ha=\{ha \mid \forall h\in H, a\in G\}.$$

例 14.10.3 在三次对称群 $S_3=\{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$ 中，$H=\{(1),(1\ 2)\}$ 是它的一个子群，则它们元素间的等价关系：

$(1)\sim(1\ 2)$，因为 $(1)\cdot(1\ 2)^{-1}=(1\ 2)\in H$.

$(1\ 3) \sim (1\ 2\ 3)$，因为 $(1\ 3)(1\ 2\ 3)^{-1} = (1\ 3)(3\ 2\ 1) = (1\ 2) \in H$.

$(2\ 3) \sim (1\ 3\ 2)$，因为 $(2\ 3)(1\ 3\ 2)^{-1} = (1\ 2) \in H$.

$(1) \nsim (1\ 3)$，因为 $(1)(1\ 3)^{-1} = (1\ 3) \notin H$.

$(1\ 3) \nsim (2\ 3)$，因为 $(1\ 3)(2\ 3)^{-1} = (1\ 2\ 3) \notin H$.

从而 S_3 被 H 分成以下三个右陪集：$S = \{H(1), H(1\ 3), H(2\ 3)\}$，其中

$$H(1) = H(1\ 2) = \{(1), (1\ 2)\},$$
$$H(1\ 3) = H(1\ 2\ 3) = \{(1\ 3), (1\ 2\ 3)\},$$
$$H(2\ 3) = H(1\ 3\ 2) = \{(2\ 3), (1\ 3\ 2)\}.$$

这三个右陪集亦可以直接利用 S_3 的元素右乘 H 的各元素得到.

与右陪集相应，可以建立左陪集的概念.

定理 14.10.4 设 H 是群 G 的子群，则利用 H 建立的群 G 的元素间的关系 $\sim'$：

$$\forall a, b \in G,\ a \sim' b \Leftrightarrow b^{-1}a \in H.$$

是一个等价关系.

定义 14.10.5 由等价关系"$\sim'$"所决定的集叫做子群 H 的**左陪集**(left coset). a 所在的左陪集用 aH 表示.

定理 14.10.6 设 H 是群 G 的子群，$a \in G$，则 H 的左陪集是 $aH = \{ah \mid \forall h \in H, a \in G\}$.

例 14.10.7 S_3 的三个左陪集是

$(1)\ \ H = \{(1), (1\ 2)\} = (1\ 2)H$,

$(1\ 3)\ H = \{(1\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H$,

$(2\ 3)\ H = \{(2\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H$.

所以 S_3 的左陪集分解是：

$$S_3 = \{(1)H, (1\ 3)H, (2\ 3)H\}.$$

注意：同一元素所在的左陪集与它所在的右陪集未必相等，如$(1\ 3)H \neq H(1\ 3)$，$(2\ 3)H \neq H(2\ 3)$.

定理 14.10.8 一个子群 H 的右陪集的个数 S_r 和它的左陪集的个数 S_l 是相等的.(它们或者都是无限大,或者都是有限并且相等.)

定义 14.10.9 群 G 的一个子群 H 的右陪集(或左陪集)的个数叫做 H 在 G 中的**指数**(index).

定理 14.10.10 Lagrange 定理 设 H 是有限群 G 的一个子群,则 H 的阶 n 和它在 G 中的指数 j 都能整除 G 的阶 N,而且

$$N = nj.$$

定理 14.10.11 有限群 G 的任一元素 a 的阶都能整除 G 的阶.

例 14.10.12 以 S_3 和 $H=\{(1),(1,2)\}$ 为例说明上面两个定理:S_3 的阶是 6,H 的阶是 2,H 有三个右(左)陪集,所以 H 的指数是 3,2 和 3 都能整除 6,并且 $6=2\times3$.

S_3 的 6 个元素的阶分别是 1,2 和 3,它们都能整除 6.

14.10.2 正规子群与商群

利用群 G 的子群 H 构成的左、右陪集 aH 及 Ha 未必相等.这在例 14.10.7 中已经看到了,因而不能利用它们构成新群.本节将讨论一种特殊的子群,利用它可以构成一个商群,通过商群可以观测到原群的某些性质.

定义 14.10.13 群 G 的子群 N,若对于 $\forall a\in G$,都有

$$Na = aN,$$

则称 N 是 G 的**正规子群(或不变子群)**(normal subgroup-invariant subgroup).

定义 14.10.14 群 G 的正规子群 N 的一个左(或右)陪集叫

做 N 的一个**陪集**(coset).

例 14.10.15 (1) 群 G 本身及由单元 e 组成的子群 $\{e\}$ 是 G 的正规子群.

(2) 设 H 由 G 中所有能与 G 的每个元素 g 交换的元素 n 组成:

$$N = \{n \in G \mid \forall g \in G \text{ 都有 } gn = ng\}.$$

则可证 N 是 G 的一个正规子群,称为群 G 的**中心**(center).

(3) 交换群 G 的每个子群 H 都是 G 的正规子群.

(4) 在三次对称群 S_3 中,$H_1=\{(1),(1\ 2)\}$,$H_2=\{(1),(1\ 3)\}$,$H_3=\{(1),(2\ 3)\}$ 及 $A_3=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$ 都是它的真子群,但前三个都不是正规子群,只有 A_3 是它的正规子群.这个正规子群由 S_3 的所有"偶"置换构成,特称为**三次交代群**(alternating group)A_3.

下面是关于正规子群的重要定理,可以用于检验正规子群.

定理 14.10.16 设 N 是群 G 的子群,则以下的命题是等价的:

(1) N 是 G 的不变子群;

(2) $\forall a \in G: aNa^{-1} = N$;

(3) $\forall a \in G: aNa^{-1} \subseteq N$;

(4) $\forall a \in G$ 及 $\forall n \in N: ana^{-1} \in N$.

设群 $G=\{a,b,c,\cdots\}$ 及它的正规子群 N 已给定,根据群的分解理论,G 被 N 分成若干个陪集,它们构成族:

$$\pi_N = G/N = \{aN, bN, cN, \cdots\}.$$

如在 G/N 上规定运算"$\circ$"如下:

$$(xN) \circ (yN) = (x \circ y)N,$$

则 G/N 关于运算"$\circ$"构成群.

定义 14.10.17 群 $\langle G; \cdot \rangle$ 的正规子群 $\langle N; \cdot \rangle$ 的陪集族

$G/N=\{aN, bN, \cdots\}$关于陪集的运算"$\circ$"构成的群$\langle G/N;\circ\rangle$称为G关于N构成的**商群**(quotient group).

例 14.10.18 三次对称群S_3由三次交代群A_3(见例14.10.15)构成的两个陪集是

$(1)A_3=A_3(1)=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$,

$(1\ 2)A_3=A_3(1\ 2)=\{(1\ 2),(1\ 3),(2\ 3)\}$.

所以,$S_3/A_3=\{(1)A_3,(1\ 2)A_3\}$.

其运算表如表 14.13.

表 14.13

$\circ$	$(1)A_3$	$(1\ 2)A_3$
$(1)A_3$	$(1)A_3$	$(1\ 2)A_3$
$(1\ 2)A_3$	$(1\ 2)A_3$	$(1)A_3$

14.11 群的同态与同构

在 14.4 节中介绍过的有关半群的同态和同构的概念及结论,都可以应用到群与含更多个运算的代数结构上去.本节除介绍群的同态的一般性质外,还介绍群和它的商群之间存在的同态关系以及利用同态映射的核制作出与群的同态像同构的商群.

定理 14.11.1 设$\langle G;\cdot\rangle$是群,$\langle G';\cdot'\rangle$是一个代数结构,若在它们间存在一个同态满射(或同态)φ:

$$\langle G;\cdot\rangle \sim \langle G';\cdot'\rangle,$$

则$\langle G';\cdot'\rangle$也是一个群.

上述定理说明群G的同态像$G'=\varphi(G)$是一个群,但群G的同态逆像未必是群.

定理 14.11.2 设G及G'是两个同态的群,$G\sim G'$在同态满

射 φ 之下，G 的单元 e 的像 $\varphi(e)$ 是 G' 的单元 e'，G 的元素 a^{-1} 的像 $\varphi(a^{-1})$ 是 a_1 的像 $\varphi(a)$ 的逆元，即

$$\varphi(e) = e',$$

$$\varphi(a^{-1}) = (\varphi(a))^{-1}.$$

定义 14.11.3 设 φ 是集 A 到集 A' 的满射，集合 $S \subseteq A$，$S' \subseteq A'$：

$$S' = \{\varphi(s) \mid s \in S\},$$

$$S = \{s \mid \varphi(s) = s', s' \in S'\},$$

则称 S' 是 S 在 φ 下的像(集)；S 是 S' 在 φ 下的**逆像集**.

定理 14.11.4 设 G 和 G' 是两个群，并且 G 与 G' 同态，则在此同态满射 φ 下：

(1) G 的子群 H 的像 $\varphi(H)$ 是 G' 的子群；

(2) G 的正规子群 N 的像 $\varphi(N)$ 是 G' 的正规子群.

定理 14.11.5 设 G 和 G' 是两个群，并且 G 与 G' 同态，则在此同态满射 φ 下：

(1) G' 的子群 H' 的逆像 H 是 G 的子群；

(2) G' 的正规子群 N' 的逆像 N 是 G 的正规子群.

综合上述两定理，群的子群和正规子群不受同态满射影响.

以下介绍著名的群的同态基本定理，为了加深理解分两部分叙述：

定理 14.11.6 任意群 G 都同它的商群 G/N 同态：

$$G \sim G/N.$$

为了给出基本定理的第二部分，需介绍同态映射的核的概念.

定义 14.11.7 设 φ 是群 G 到群 G' 的同态映射，G' 的单元 e' 在 φ 之下的所有逆像构成的 G 中的子集叫做同态映射 φ 的核(kernel)用 $\ker\varphi = \{g \mid g \in G, \varphi(g) = e'\}$ 表示.

定理 14.11.8 设 G 和 G' 是两个群，并且 G 与 G' 在 φ 下同态，则该同态映射的核 $N = \ker\varphi$ 是 G 的一个正规子群，而且

$$G/\ker\varphi \cong G'.$$

将定理 14.11.6，定理 14.11.8. 合并即得如下定理.

定理 14.11.9　群的同态基本定理(fundamental theorem of homomorphism)　任何群 G 的商群都是 G 的一个同态像；反之，若群 G' 是群 G 的一个同态像，则 G' 必同构于 G 的一个商群.

例 14.11.10　(1) 设 $G=\langle \mathbf{R};+\rangle$ 为实数加群，$G'=\langle\{e^{i\theta}\mid 0\leqslant\theta<2\pi\};\cdot\rangle$ 是模为 1 的复数乘群. 作映射 $\varphi:\theta\mapsto e^{i\theta}$，则可证 φ 是 G 到 G' 的一个同态满射：$G\sim G'$. 此时 $\ker\varphi=\langle 2\pi\rangle$（$2\pi$ 生成的循环群）. 所以

$$G/\langle 2\pi\rangle\cong G'.$$

(2) 令 $G=\langle \mathbf{Z}_{12};+\rangle$ 为模 12 的同余类加群；$G'=\langle\{1,i,-1,-i\};\cdot\rangle$ 为四次单位根乘群. 在 G 与 G' 间作映射 φ

$$\varphi:\quad \left.\begin{array}{l}[0]\\ [4]\\ [8]\end{array}\right\}\mapsto 1 \qquad \left.\begin{array}{l}[1]\\ [5]\\ [9]\end{array}\right\}\mapsto i$$

$$\left.\begin{array}{l}[2]\\ [6]\\ [10]\end{array}\right\}\mapsto -1 \qquad \left.\begin{array}{l}[3]\\ [7]\\ [11]\end{array}\right\}\mapsto -i$$

则可证 φ 是 G 与 G' 间的同态满射，且

$$\ker\varphi=\{[0],[4],[8]\}=N.$$

作商群　$G/N=\{[0]+N,[1]+N,[2]+N,[3]+N\}$，

易见　　$G/N\cong G'$.

14.12　群在编码理论中的应用

14.12.1　纠错码及其有关概念

在计算机及通信系统中，信息是用二进制数字信号表示的. 这

些数字信号在传送过程中,由于各种干扰,常会产生失真现象,即可能使 0 变成 1,或使 1 变成 0,使得从发送端发出的二进制信号串 $\boldsymbol{w}=a_1a_2\cdots a_n$ 变成接收端收到的 $\boldsymbol{w}'=a_1'a_2'\cdots a_n'$(可能有某些 $a_i\neq a_i'$),可能产生二进制信号的传递错误. 为防止这种错误,有两种方法:一是提高设备及信号的抗干扰能力;二是在编码时使编出的二进制数码在传送过程中,一旦出现错误码时,在接收端设置的纠错设备能够立刻发现并将其纠正. 后者简单易行,目前已被广泛采用. 本节将介绍这些能有效提高信息保真的纠错码,特别是建立于 Lagrange 定理 14. 10. 10 基础之上的群码(group codes)和 Hamming 码.

定义 14.12.1 一个由传送符号 0 与 1 的传递器及接收器组成的信道,如果它们错误传递这两个数字的概率是相等的,那么就称它为**二进制对称信道**(binary symmetric channel).

设 0 被误传成 1 的概率为 $p(0\leqslant p\leqslant 1)$,则它被正确传送成 0 的概率为 $q=1-p$;同理,1 被误传成 0 的概率为 p,而它被传送成 1 的概率为 $q=1-p$. 这两个数字被误传的概率相等,所以称它为对称信道.

二进制对称信道示意如图 14.8.

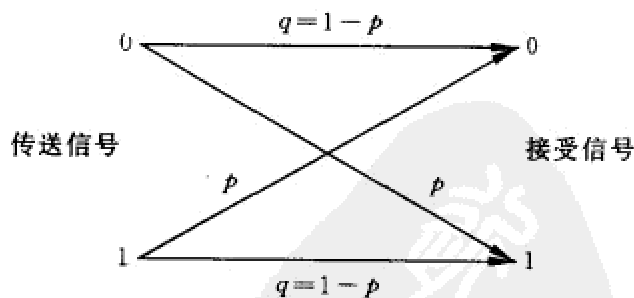


图 14.8

定义 14.12.2 设 $B_2=\{0,1\}$.

(1) 由 0,1 组成的二进制串称为**字**(word);

(2) 字的集合称为**码(集)**(code);

(3) 码中的字称为**码字**(code word);

(4) 不在码中的字称为**废码字**(useless code);

(5) 特殊的码字 0 和 1 称为**码元**(code element);

(6) 码字中码元的个数称为**码长**(code length).

例 14.12.3 集 $A=\{0,1,10,101\}$是一个码,其中 0,1 是两个长度为 1 的码字,10 是长度为 2 的码字,101 是长度为 3 的码字. 又如集 $B=\{001,100,111,010\}$也是一个码,每个码字的长度都是 3;此外长度为 3 的二进制串还有 000,011,101,110 四个,它们不属于 B 这个码,所以对 B 而言它们都是废码.

定义 14.12.4 设长度为 n 的被传送字是 $\boldsymbol{w}=w_1w_2\cdots w_n$,而接收字是 $\boldsymbol{r}=r_1r_2\cdots r_n$. 符合以下条件的字 $\boldsymbol{e}=e_1e_2\cdots e_n$ 称为一个**错误模式**(error pattern)

$$e_i=\begin{cases}0, & \text{如果 } w_i=r_i\\ 1, & \text{如果 } w_i\neq r_i\end{cases}$$

例 14.12.5 $\boldsymbol{w}=01011010$,$\boldsymbol{r}=01111011$,则

$\boldsymbol{e}=00100001$;又如 $\boldsymbol{r}=111001001000$,

$\boldsymbol{e}=000000001000$,则 $\boldsymbol{w}=111001000000$.

定理 14.12.6 (1) $\boldsymbol{e}$ 中 1 的个数是传递 $\boldsymbol{w}$ 时产生错误的个数,$\boldsymbol{e}$ 中各 1 的位置就是产生错误的位置.

(2) 设"$\oplus$"是集 $B=\{0,1\}$内的对位布尔和(即 $0\oplus0=1\oplus1=0$, $0\oplus1=1\oplus0=1$),则

$\boldsymbol{w}=\boldsymbol{r}\oplus\boldsymbol{e}$ (传送字=接收字$\oplus$错误模式);

$\boldsymbol{r}=\boldsymbol{w}\oplus\boldsymbol{e}$ (接收字=传送字$\oplus$错误模式);

$\boldsymbol{e}=\boldsymbol{w}\oplus\boldsymbol{r}$ (错误模式=传送字$\oplus$接收字).

由概率论方法可以得到以下定理.

定理 14.12.7 设通过二进制对称信道传送的长为 n 的字为 $\boldsymbol{w}$. 又设数码 0,1 产生错误的概率为 p,则

(1) 若 e 是一个包含 k 个 1 的错误模式，则 e 出现的概率为 $p^k(1-p)^{n-k}$；

(2) 含有 k 个 1 的长为 n 的错误模式共有 $\binom{n}{k}=\frac{n!}{(n-k)!\ k!}$ 个，因此在传送 w 时恰产生 k 个错误的概率为 $\binom{n}{k}p^k(1-p)^{n-k}$.

例 14.12.8 设单个码元出错的概率 $p=0.01$，现传送长为 100 的码字，则不出错的概率是

$$(1-p)^n=(1-0.01)^{100}\approx 0.36603;$$

仅出现一个错误的概率是

$$\binom{n}{1}p(1-p)^{n-1}=100(0.01)(1-0.01)^{99}\approx 0.36973;$$

出现两个错误的概率是

$$\binom{n}{2}p^2(1-p)^{n-2}=\frac{100\times 99}{2}(0.01)^2(1-0.01)^{98}\approx 0.18486;$$

出现两个以上错误的概率约为

$$1-0.36603-0.36973-0.18486=0.07938.$$

14.12.2 编码与译码

为了提高信息传送的正确性，通常总是将长为 m 的**信息字**(message word) $a_1a_2\cdots a_m$ 变成长为 n 的码字 $(m<n)$ $a_1a_2\cdots a_ma_{m+1}\cdots a_n$. 这是根据通常语言中**冗余性原则**(principle of redundancy)而采取的，因为在通常的印刷品中一个较长的字排印错误常较易发现和纠正. 这样的码 $(n>m)$ 称为 **(n,m) 信息组代码**，简称 (n,m) **分组码**(block code)，并称 $a_1a_2\cdots a_m$ 为**信息位**(information digits)，$a_{m+1}a_{m+2}\cdots a_n$ 为**校验位**(check digits). 后者是专为保证信息准确传送而设计的，对于原信息并不产生影响，所以又被称为**冗余位**(redundant digits). 如图 14.9 所示.

这些码字通过信道传送到接收器后可做以下两种工作：一是**检验错误**(detect errors)，它检验所接收到的字，是否是该码中的码字，如果是，就被认为是所传送的字；如果不是，则可肯定在传送过程中出现了错误，接收器就可以要求将该字重新传送. 另一方式是**纠正错误**(correct errors). 此时译码器选择最可能产生这个接收字的码字作为被传送的码字.



图 14.9

这个通信系统的数学模型如图 14.10 所示：

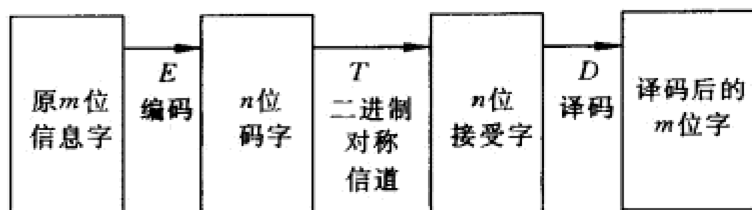


图 14.10

据此可以对它作如下的数学描述.

定义 14.12.9 一个二进制信息的(n,m)分组码是由一个**编码函数** $E:B_2^m\to B_2^n$ 及一个**译码函数** $D:B_2^n\to B_2^m$ 组成. 此二函数能使复合运算后的函数 $H=D\circ T\circ E$ 成为一个具有接近于概率 1 的恒等函数，其中 T 是由信道产生的**错误函数**(error funtion).

比值 $R=\frac{m}{n}$ 称为**码率**(code rate)或**信息率**(information rate).

例 14.12.10 (1) $(m+1,m)$奇偶校验码(parity-check code)的编码函数是：

$E:a_1\cdots a_m=a\mapsto b=b_1\cdots b_{m+1}$ 其中 $b_1=a_1$，$b_2=a_2$，…，$b_m=a_m$，而规定

$$b_{m+1} = \begin{cases} 0 & \text{若} \sum_{i=1}^{m} a_i \text{ 是偶数,} \\ 1 & \text{若} \sum_{i=1}^{m} a_i \text{ 是奇数.} \end{cases}$$

(例如,当 $m=2$ 时,E:$00 \mapsto 000, 01 \mapsto 011, 10 \mapsto 101, 11 \mapsto 110$).

由定义可见这种码的每个码字中码元 1 的个数总是一个偶数.

其译码函数 D:$\boldsymbol{b} \mapsto \boldsymbol{c}$ 定义为

$$b_i = c_i \qquad i = 1, 2, \cdots, m.$$

这种码的检错能力可利用和数 $\sum_{i=1}^{m+1} b_i$ 是否偶数来考察:如果该和是奇数,则可以肯定传送时产生了一个或奇数个错误,但不能判定是哪一位上出错;如果和数是偶数,则不能断言传送正确(因为在两位出错时这个和也是偶数).所以这种码是检错码,并且只能检查单个错误.

(2) $(3m, m)$三倍重复码(triple-repetition code)是一种常用的纠错码,其编码函数 E:$B_2^m \to B_2^{3m}$ 是将每个 m 位信息字重复三次:

$$E(a_1 a_2 \cdots a_m) = a_1 a_2 \cdots a_m a_1 a_2 \cdots a_m a_1 a_2 \cdots a_m.$$

译码函数 D:$B_2^{3m} \mapsto B_2^m$ 则将同一位上至少重复过两次的数字选作该位的码元. 例如当 $m=3$ 时,$E(010)=010010010$,如果传送时在第 6 位上出现了一个错误,使接收字变成 010011010,这时应译作 010. 因为第 1,4,7 位上全是 0;第 2,5,8 位上全是 1;第 3,9 位上是 0;而第 6 位上却是 1. 按照“多者优先”原则可认为第 6 位上出了错,应将其改为 0,这就恢复了被传送码字的原形 101.

所以此码能自动纠正所有的单个错误,它是纠单错码.

(3) $(5m, m)$五倍重复码(five-time-repetition code)其编码和

译码函数与(2)类似,只是将每个码字重复五次,它能纠正两个错误,是纠双错码.

(4) 为了说明定义 14.12.9 中"使 $H=D\circ T\circ E$ 成为一个具有接近于概率 1 的恒等函数"以及对比各种码的优越性.考察上面三种码无错传送的概率:设单个字符错传的概率为 0.001,则用奇偶校验码处理一个有 1 万个位的信息时,其不出错的概率经计算约为 0.946,此时共需传送 10001 个字符;若用三倍重复码,其不出错的概率约为 0.97,此时共需传送 3 万个字符;若用五倍重复码,此概率可提高到 0.9999,但此时却要传送 5 万个字符.如果不经过编码处理,由概率计算可知,传送 1 万个字符而不出错的概率等于 $(1-0.001)^{10000}\approx 0.00005$,即约为十万分之五!由此可见,在传送信息时进行编码对于提高信息准确性与传送效率有极大的作用.

14.12.3 码的检错及纠错能力

定义 14.12.11 码字 $\boldsymbol{a}=a_1a_2\cdots a_n$ 的**重**(weight)$w(\boldsymbol{a})$是指它所含码元 1 的个数.

定义 14.12.12 设 $\boldsymbol{a}=a_1a_2\cdots a_n$ 与 $\boldsymbol{b}=b_1b_2\cdots b_n$ 是两个等长的码字,则它们的对位布尔和$\oplus$的重称为码字 $\boldsymbol{a}$ 与 $\boldsymbol{b}$ 之间的 **Hamming 距离**(distance).简称 $\boldsymbol{a}$ 与 $\boldsymbol{b}$ 之间的**距离**.用 $d(\boldsymbol{a},\boldsymbol{b})$ 表示.

按对位布尔和$\oplus$的定义:当 $a_i=b_i$ 时 $a_i+b_i=0$;而当 $a_i\neq b_i$ 时 $a_i+b_i=1$.故 $d(\boldsymbol{a},\boldsymbol{b})=w(\boldsymbol{a}\oplus\boldsymbol{b})$.它实际是 $\boldsymbol{a}$ 与 $\boldsymbol{b}$ 中 $a_i\neq b_i$ 的位的个数.

定义 14.12.13 给定一个码 C 后,C 中所有不同码字之间的 Hamming 距离的最小值称为码 C 的**最小距离**(minimum distance),用 $d_{\min}(C)$表示.

例 14.12.14 设码 $C=\{0000,0011,1001,1011\}$,则 $w(0000)=0$,

$w(0011)=w(1001)=2, w(1011)=3$；而 $d(0000,0011)=w(0000 \oplus 0011)=w(0011)=2$. 同理，$d(0000,1001)=2$，$d(0000,1011)=3$，$d(0011,1001)=2$，$d(0011,1011)=1$，$d(1001,1011)=1$，因此 $d_{\min}(C)=1$.

定理 14.12.15 设 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\in C$，则有

(1) $d(\boldsymbol{a},\boldsymbol{a})=0$；

(2) $d(\boldsymbol{a},\boldsymbol{b})=d(\boldsymbol{b},\boldsymbol{a})$；

(3) $d(\boldsymbol{a},\boldsymbol{b})+d(\boldsymbol{b},\boldsymbol{c})\geqslant d(\boldsymbol{a},\boldsymbol{c})$；

(4) $d(\boldsymbol{a}\oplus\boldsymbol{c},\boldsymbol{b}\oplus\boldsymbol{c})=d(\boldsymbol{a},\boldsymbol{b})$.

定理 14.12.16 码 C 能检出所有重 $\leqslant k$ 的错误模式的充要条件是 $d_{\min}(C)\geqslant k+1$.

由定义 14.12.4 及定理 14.12.6 可知，由错误模式可以决定传送时所产生错误的个数及位置. 因此，定理则说：码 C 能检出不超过 k 个错误的充要条件是

$$d_{\min}(C)\geqslant k+1.$$

定理 14.12.17 码 C 能纠正所有重 $\leqslant k$ 的错误模式的充要条件是 $d_{\min}(C)\geqslant 2k+1$.

或码 C 能纠正 k 个错误的充要条件是 $d_{\min}(C)\geqslant 2k+1$.

例 14.12.18 (1) 令 $C_1=\{00,11\}$，则由 $d_{\min}(C_1)=2$，故可检出一个错误.

(2) (3,1)三倍重复码 $C_2=\{000,111\}$ 的 $d_{\min}(C_2)=3$，故可纠正一个错误及检出两个以内的错误.

(3) 令 $C_3=\{00,01,10,11\}$，它包含了所有长度为 2 的码字. 因 $d_{\min}(C_3)=1$，它不能检查出任何错误. 这是因为码 C_3 包含了全部长度为 2 的码字，当其中一个码元被传错时就变成 C_3 中的另一个码字，因此无法判断是否出了错误. 由此可见，一个码若包含了某长度的所有码字，则此种码必无检错和纠错能力.

(4) (3,2)奇偶校验码 $C_4=\{000,011,101,110\}$，因 $d_{\min}(C_4)=$

2,故可检出一个错误但不能纠正错误.

(5) (5,1)五位重复码 $C_5=\{00000,11111\}$,因 $d_{\min}(C_5)=5$. 所以它能检出 4 个错误及纠正 2 个错误.

现将几种常用码的检错和纠错能力列成表 14.14.

表 14.14

码名	码的最小距离 $d_{\min}(C)$	检错个数	纠错个数	信息率 m/n
(3,2)奇偶检验码	2	1	0	$\frac{2}{3}$
(3,1)三倍重复码	3	2	1	$\frac{1}{3}$
(5,1)五倍重复码	5	4	2	$\frac{1}{5}$
(n,m)码	d	$d-1$	$\leqslant\frac{d-1}{2}$	$\frac{m}{n}$

14.12.4 利用矩阵及群进行编码及译码

前述几种码的编码函数 E 及译码函数 D 都是通过语言描述或列表法(字典)给出的,这些方法既繁琐又不便于作深入研究.本节介绍利用矩阵及群两种代数工具进行编码及译码,它们是方便而有力的编码工具.

定义 14.12.19 设 $m<n$. $\boldsymbol{G}_{m\times n}$是 $B_2=\{0,1\}$上的矩阵,若它的前 m 行,m 列的元素构成一个单位方阵 $\boldsymbol{I}_m$,则称它是**生成矩阵**(generator matrix).

定理 14.12.20 利用一个 $m\times n$ 的生成矩阵 $\boldsymbol{G}_{m\times n}$可以确定一个$(n,m)$信息组代码的编码函数 $E:B_2^m\to B_2^n$. 如下:

$$\forall \boldsymbol{a}=a_1a_2\cdots a_m\in B_2^m,令\ E(\boldsymbol{a})=\boldsymbol{a}\boldsymbol{G}_{m\times n}.$$

(**注意**:定理中的 $\boldsymbol{a}\boldsymbol{G}_{m\times n}$表示码字 $\boldsymbol{a}$ 与矩阵 $\boldsymbol{G}_{m\times n}$的乘积,而码字 $\boldsymbol{a}$ 视作 m 元行向量!)

例 14.12.21

令

$$G_{3\times 6}=\begin{bmatrix}1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix},$$

则 $G_{3\times 6}$ 是一个生成矩阵，由它可以确定一个(6,3)信息组代码. 它的编码函数 E 用矩阵表示如下：

$$E(w)=w\begin{bmatrix}1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix}.$$

现在由各信息字具体计算它的码字如下：(6,3)码的信息字总共有 8 个，它们构成 $B_2^3=\{000,001,010,011,100,101,110,111\}$，与它们相应的码字是：

$$E(000)=000\begin{bmatrix}1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix}=000000,$$

$$E(001)=001\begin{bmatrix}1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix}=001011.$$

同理可得

$$\begin{aligned}E(010)&=010G_{3\times 6}=010101,\\E(011)&=011G_{3\times 6}=011110,\\E(100)&=100G_{3\times 6}=100110,\\E(101)&=101G_{3\times 6}=101101,\\E(110)&=110G_{3\times 6}=110011,\\E(111)&=111G_{3\times 6}=111000.\end{aligned}$$

由上可见，利用生成矩阵编码是非常方便的. 因为仅须用到矩阵乘法，它们可由计算机来完成. 当传送正确时，它的破译也很容

易，因为 G 的前 m 行，m 列的元素构成单位方阵，它的信息字恰好就是码字的前 m 位；但当传送有错时，纠正这个错误恢复原来的信息字就不能仅靠使用生成矩阵了，还要配合使用下面矩阵.

定义 14.12.22 设 $m<n$，$\boldsymbol{H}_{(n-m)\times n}$ 是 $B_2=\{0,1\}$ 上的矩阵，若它的后 $n-m$ 行与 $n-m$ 列元素构成单位方阵 $\boldsymbol{I}_{(n-m)}$. 则称 $\boldsymbol{H}_{(n-m)\times n}$ 是一个**奇偶校验矩阵**(parity-check matix).

定理 14.12.23 每个奇偶校验矩阵 $\boldsymbol{H}_{(n-m)\times n}$ 确定唯一的 (n,m) 信息分组代码的编码函数 $E:B_2^m\to B_2^n$，它对于每个信息字 $\boldsymbol{w}=a_1a_2\cdots a_m\in B_2^m$ 通过下列条件确定码字 $E(\boldsymbol{w})=a_1a_2\cdots a_ma_{m-1}\cdots a_n\in B_2^n$：

(1) $E(\boldsymbol{w})$ 的前 m 位与 $\boldsymbol{w}$ 的前 m 位相同，

(2) $E(\boldsymbol{w})$ 的其余 $n-m$ 位码元由以下的名为**奇偶校验方程**(parity-check equation)的矩阵方程：

$$\boldsymbol{H}\cdot E(\boldsymbol{w})^{\mathrm{T}}=\boldsymbol{0}$$

的解，它是一个含有 $n-m$ 个方程式的方程组，而以前 m 个码元 $a_1,a_2,\cdots,a_m$ 为参数.

例 14.12.24 同例 14.12.21 中的(6,3)分组码，其生成矩阵为

$$\boldsymbol{G}_{3\times 6}=\begin{bmatrix}1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix},$$

则其校验矩阵

$$\boldsymbol{H}_{3\times 6}=\begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix}.$$

任取 $\boldsymbol{w}=a_1a_2a_3\in B_2^3$，则 $E(\boldsymbol{w})=a_1a_2a_3a_4a_5a_6$，其中 a_4,a_5,a_6 由奇偶校验方程 $\boldsymbol{H}\cdot E(\boldsymbol{w})^{\mathrm{T}}=\boldsymbol{0}$ 决定，即

$$\begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix}\cdot\begin{bmatrix}a_1\\a_2\\a_3\\a_4\\a_5\\a_6\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix}.$$

展开得方程组[①]

$$\begin{cases}a_1+a_2+a_4=0,\\a_1+a_3+a_5=0,\\a_2+a_3+a_6=0.\end{cases}$$

即

$$\begin{cases}a_4=a_1+a_2,\\a_5=a_1+a_3,\\a_6=a_2+a_3.\end{cases}$$

用 B_2^3 中 8 个码字 000,001,…,111 的相应码元代入即可得到与例 14.12.21 相同的结果.

由定理 14.12.23 中编码函数 E 的唯一性可得以下定理.

定理 14.12.25 设 $\boldsymbol{u}$ 是以信息字 $\boldsymbol{w}$ 为前 m 个码元的码字,且满足 $\boldsymbol{H}\boldsymbol{u}^{\mathrm{T}}=\boldsymbol{0}$,则 $\boldsymbol{u}=E(\boldsymbol{w})$.

换言之,满足此二条件的码字 $\boldsymbol{u}$ 就是与 $\boldsymbol{w}$ 相对应的码字.

还可以利用奇偶校验矩阵 $\boldsymbol{H}$ 检查编码所出现的错误:设码字为 $\boldsymbol{c}$,由定理14.12.25有 $\boldsymbol{H}\cdot\boldsymbol{c}^{\mathrm{T}}=\boldsymbol{0}$,又设在传送过程中它的第 i 位出现错误,则接收字 $\boldsymbol{r}=\boldsymbol{c}\oplus\boldsymbol{e}_i$,这里的 $\boldsymbol{e}_i=\overbrace{\underbrace{00\cdots01}_{i\text{ 个位}}0\cdots0}^{n}$ 是一个错误模式见定理 14.12.6,因而 $\boldsymbol{H}\cdot\boldsymbol{r}^{\mathrm{T}}=\boldsymbol{H}\cdot(\boldsymbol{c}\oplus\boldsymbol{e}_i)^{\mathrm{T}}=\boldsymbol{H}\cdot\boldsymbol{c}^{\mathrm{T}}\oplus\boldsymbol{H}\cdot\boldsymbol{e}_i^{\mathrm{T}}=\boldsymbol{H}\cdot\boldsymbol{e}_i^{\mathrm{T}}=\boldsymbol{H}_{\cdot i}$($\boldsymbol{H}$ 的第 i 个列向量).

---

① 方程组中码元 a_i、a_j 间的"加法"是对位布尔和,即 $a_i=a_j$ 时,$a_i+a_j=0$;$a_i\neq a_j$ 时,$a_i+a_j=1$.

反之,若 $\boldsymbol{H}\cdot\boldsymbol{r}^{\mathrm{T}}=\boldsymbol{H}_{\cdot i}$,则接收字 $\boldsymbol{r}$ 的第 i 位上的码元有错.将它改正后即可得出正确码字 $\boldsymbol{c}$.

因此有下面的定义.

定义 14.12.26 设 $\boldsymbol{H}$ 是一个奇偶校验矩阵,$\boldsymbol{r}$ 是一个接收字,则 $\boldsymbol{S}=\boldsymbol{H}\cdot\boldsymbol{r}^{\mathrm{T}}$ 称为字 $\boldsymbol{r}$ 的**校验子**(syndrome).

定理 14.12.27 设接收字为 $\boldsymbol{r}=r_1r_2\cdots r_mr_{m+1}\cdots r_n$,作它的校验子 $\boldsymbol{S}=\boldsymbol{H}\cdot\boldsymbol{r}^{\mathrm{T}}$,则:

(1) 若 $\boldsymbol{S}=\boldsymbol{0}$,则传送很可能是正确的,可以认为 $\boldsymbol{r}$ 就是所求的码字,而原来的信息字就是 $r_1r_2\cdots r_m$.

(2) 若 $\boldsymbol{S}$ 是 $\boldsymbol{H}_{\cdot i}$(列上各码元当然不能全为零),则很可能在第 i 位上产生了单错,将 $\boldsymbol{r}$ 的 r_i 纠正即得码字 $\boldsymbol{c}$,取其前 m 位即得原信息字.

(3) 若 $\boldsymbol{S}$ 既非 $\boldsymbol{0}$ 又非 $\boldsymbol{H}_{\cdot i}$,则信息字在传送中至少产生了两个错误,此时没有任何高效的破译方法(侥幸的是,当单个码元出错的概率 p 很小时,该情况是很少发生的).

例 14.12.28 (1) 仍以例 14.12.21 的(6,3)分组码为例,检验它的码字的校验字,例如 101101.由于此码的生成矩阵为

$$\boldsymbol{G}_{3\times 6}=\begin{bmatrix}1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix},$$

其奇偶检验矩阵为

$$\boldsymbol{H}_{3\times 6}=\begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix},$$

此时 101101 的校验子为

$$S = H \cdot r^{\mathrm{T}} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

可见这个码字是正确的.

(2) 设上面码字在传送时第 3 位发生错误,因而接收字 $r=100101$,现计算它的校验子

$$S = H \cdot r^{\mathrm{T}} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = H_{\cdot 3},$$

此时 S 是 $H_{\cdot 3}$(即第 3 列元素),故知接收字的第 3 位有错.将它改正后即得所传送的码字是 101101,而原信息字是 101.

(3) 设码字 101101 出现两个错误,不妨设是第 3,5 两位,相应的错误模式是 $e_{3,5}=001010$,因而接收字是 100111,它的校验子是

$$S = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = H_{\cdot 6},$$

这是 H 的第 6 列,可猜测错误出在第 6 位,据此改正后的码字 100110 虽在码中,但却不是原来传送的码字(101101).

另设错误出在第 2,5 两位上,相应的接收字是 111111,其校

验子为

$$S=\begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix}\begin{bmatrix}1\\1\\1\\1\\1\\1\end{bmatrix}=\begin{bmatrix}1\\1\\1\end{bmatrix},$$

这个校验子不是 $\boldsymbol{H}_{\cdot i}$，但它是 $\boldsymbol{H}$ 的第 1 列与第 6 列之和，或是第 2 列与第 5 列的和. 或是第 3 列与第 4 列之和，经检验仅有第 2 种猜测（错误出在第 2,5 列）是正确的.

由此可见，对出现双错的破译常常会产生错误，不一定能得出正确的译码.

定理 14.12.29 奇偶校验矩阵 $\boldsymbol{H}_{(n-m)\times n}$ 能够正确破译所有单个错误的充要条件是 $\boldsymbol{H}_{(n-m)\times n}$ 的各列都是非全部为零的及相异的向量.

同一个码的生成矩阵与奇偶检验矩阵之间存在着密切的关系，可从下面的定理看出.

定理 14.12.30 （1）若 $\mathbf{A}$ 是 B_2 上的一个 $m\times(n-m)$ 矩阵，因而 $\boldsymbol{G}_{m\times n}=[\boldsymbol{I}_m,\mathbf{A}]$ 是一个 (n,m) 分组码的生成矩阵，则 $\boldsymbol{H}_{(n-m)\times n}=[\boldsymbol{A}^{\mathrm{T}},\boldsymbol{I}_{n-m}]$ 是这同一个码的奇偶校验矩阵；

（2）若 $\boldsymbol{B}$ 是 B_2 上的一个 $(n-m)\times m$ 矩阵，因而 $\boldsymbol{H}_{(n-m)\times n}=[\boldsymbol{B},\boldsymbol{I}_{n-m}]$ 是一个 (n,m) 分组码的奇偶校验矩阵. 则 $\boldsymbol{G}_{m\times n}=[\boldsymbol{I}_m,\boldsymbol{B}^{\mathrm{T}}]$ 是这同一个码的生成矩阵.

注意：$[\boldsymbol{I}_m,\mathbf{A}]$ 是分块矩阵，余同.

下面利用群的理论来研究编码和译码.

主要利用 Lagrange 有关陪集的定理 14.10.10.

定理 14.12.31 （1）长为 m 的信息字集合 B_2^m 关于对位布尔和 $\oplus$ 构成加群；

(2) 长为 n 的码字集合 B_2^n 关于对位布尔和$\oplus$也构成加群.

定理 14.12.32 由任意生成矩阵 $\boldsymbol{G}$ 或奇偶校验矩阵 $\boldsymbol{H}$ 确定的编码函数 $E: B_2^m \to B_2^n$ 是一个由信息字加群 B_2^m 到码字加群 B_2^n 的单态射,且知由 $\boldsymbol{G}$ 与 $\boldsymbol{H}$ 得到的码 $\boldsymbol{c}$(参看定理 14.12.30)构成 B_2^n 的子群.

定义 14.12.33 如果一个分组码的所有码字构成一个加群[①],则称该码为**群码**(group code).

定理 14.12.34 由任意生成矩阵或奇偶校验矩阵得到的码必为群码.

前面已经看到,一个码的检错与纠错能力完全取决于两个码字间的最小距离,对于群码来说,这个距离很易求出,因为有以下定理.

定理 14.12.35 在一个群码中,码字间的最小距离等于所有非零码字的重的最小值.

今后在计算码的最小距离时,只需将码中各码字的重都计算出来,其中最小的重即为所求的最小距离.

下面介绍利用群的陪集分解进行译码的方法.每个群 G 都可以按子群 H 分解成若干个陪集,使得 G 中的每个元素恰好属于一个陪集.元素 a 所在的陪集 $a+H=\{a+h \mid h\in H\}$,它的元素是由 a"加"上 H 的每个元素得到的.

由定理 14.12.32 知群码 $\boldsymbol{c}$ 既然构成接收字群 B_2^n 的一个子群,而且是有限群,由 Lagrange 定理,B_2^n 被分解成若干个陪集,每个陪集中的接收字 $\boldsymbol{r}$ 与码 $\boldsymbol{c}$ 中的对应码字 $\boldsymbol{w}$ 仅差一个元素 $\boldsymbol{e}$,因而 $\boldsymbol{r}=\boldsymbol{w}\oplus\boldsymbol{e}$,这意味着码字 $\boldsymbol{r}$ 在传送过程中产生了错误 $\boldsymbol{e}$,若事先有意识地取 $\boldsymbol{e}$ 为错误模式,则很容易检出错误所在的位置及其个数,进而加以改正.陪集译码表的作法如下.

---

① 加群的"加法"是对位布尔和$\oplus$.

表 14.12.36　译码表(decoding table)作法

(1) 将群 $\boldsymbol{C}$ 的所有码字写在第 1 行上并将 $\mathbf{0}=\underbrace{00\cdots0}_{n}$写在该行的最左端;

(2) 将错误模式 $\boldsymbol{e}_1=\underbrace{10\cdots0}_{n}$写在第 2 行的最左端,并将它与第 1 行的各码字相加之(对位布尔)和写在对应码字的下方构成第 2 行,其全体构成陪集 $\boldsymbol{e}_1\oplus\boldsymbol{C}$.

(3) 将错误模式 $\boldsymbol{e}_2=\underbrace{010\cdots0}_{n}$写在第 3 行最左端,仿上法在第 3 行上写下陪集 $\boldsymbol{e}_2\oplus\boldsymbol{C}$ 的所有元素.

仿上一直做下去. 由于 B_2^n 与 $\boldsymbol{C}$ 都是有限群,据 Lagrange 定理,陪集个数也是有限的. 所以上述步骤经有限步后必然停止. 由陪集性质,接收字群 B_2^n 的每个元 $\boldsymbol{r}$ 恰在一个陪集之中. 它是第 1 行中群 $\boldsymbol{C}$ 的码字 $\boldsymbol{w}$ 与某一个错误模式 $\boldsymbol{e}_i$ 之和,故 $\boldsymbol{r}$ 可译成 $\boldsymbol{w}$.

(4) 为了标志各陪集及便于计算机处理,在表中各行外的最左端再加写与该行相应的校验子 $\boldsymbol{S}$ 的转置矩阵. 这是因为定理 14.12.37 的启示.

定理 14.12.37　设 $\boldsymbol{C}=\{\boldsymbol{C}\in B_2^n \mid \boldsymbol{HC}^{\mathrm{T}}=\mathbf{0}\}$是由奇偶校验矩阵 $\boldsymbol{H}$ 生成的群码,则 B_2^n 的两个字 $\boldsymbol{x},\boldsymbol{y}$ 在同一陪集中的充要条件是它们有相同的校验子:$\boldsymbol{Hx}^{\mathrm{T}}=\boldsymbol{Hy}^{\mathrm{T}}$.

定义 14.12.38　表 14.15 每行的陪集中最左端的、重量最小的码字称为该陪集的**陪集头**(leader coset).

例 14.12.39　求作例 14.12.21 的译码表,并破译以下各接收字:110110,001111,101111,101010,101000,001000,011110.

解　因为接收字群 B_2^6 的阶$=2^6=64$,而(6,3)分组码群 $\boldsymbol{C}$ 的阶是 8,由 Lagrange 定理,陪集个数$=\boldsymbol{C}$ 在 B_2^6 中的指数$=64/8=8$,故译码表应有 8 行 8 列(表外最左列是各校验子的转置矩阵),作表 14.15.

要破译以上 7 个接收字可先在表 14.15 中找到它们,然后再

在与该字同列的第 1 行上的码字就是该字的译码.(例如接收字 110110(位于第 3 行,第 1 列),在该列(第 1 列)的第 1 行上的码字是 100110,就是它的译码).余仿此,因此它们是 100110,001011,101101,001011,111000,000000,011110.删掉这些码字的后三位(校验位)即可得到原来的信息字:100,001,101,001,111,000,011.

表 14.15

校验子	陪集头	字						
000	000000	**100110**	010101	001011	110011	101101	011110	111000
110	100000	000110	110101	101011	010011	001101	111110	011000
101	010000	**110110**	000101	011011	100011	111101	001110	101000
011	001000	101110	011101	000011	111011	100101	010110	110000
100	000100	100010	010001	001111	110111	101001	011010	111100
010	000010	100100	010111	001001	110001	101111	011100	111010
001	000001	100111	010100	001010	110010	101100	011111	111001
111	100001	000111	110100	101010	010010	001100	111111	011001

以上译码法称为**利用陪集头译码法**(decoding using coset leaders),它可使每个接收字得到破译.甚至还可以应用到**纠多错码**(multiple-error-correcting code)上去,它的优越性表现在以下定理 14.12.40.

定理 14.12.40 设接收字 $\boldsymbol{r}$ 用陪集头译码法译得的码字为 $\boldsymbol{c}$,而用其他方法译出的码字为 $\boldsymbol{b}$,则 $d(\boldsymbol{r},\boldsymbol{c})\leqslant d(\boldsymbol{r},\boldsymbol{b})$.

这种译码法出错的概率不会超过其他译法出错的概率,它是一种较好的译码法.

14.12.5 Hamming 码

下面的编码是 R. W. Hamming 根据定理 14.12.29 的原理巧

妙设计的，它是一种能检单个错误的**完全码**(perfect code). 由于定理 14.12.29 及二进制数的横写习惯，在这里利用生成矩阵来表述.

算法 14.12.41　Hamming 编码法

(1) 给定正整数 r 后，令 $n=2^r-1$，$m=(2^r-1)-r$，则与 r 相应的 Hamming 码是一个(n,m)分组码.

(2) 该码的码字 $\boldsymbol{b}=b_1b_2\cdots b_n$ 的各位上的码元如下安排：b_{2^0}，b_{2^1}，b_{2^2}，…，$b_{2^{(r-1)}}$(共 r 个)是校验位上的码元，其值由下面的(4)中的方程组确定；b_3，b_5，b_6，…，b_n(共 m 个)则依次是所给信息字各位上的码元. 例如当 $r=3$ 时，$n=2^r-1=7$，$m=(2^r-1)-r=4$，这个(7,4)分组码的任意码字 $\boldsymbol{b}=b_1b_2b_3b_4b_5b_6b_7$ 的 b_1，b_2，b_4 是校验位上的码元，其余码元则是所给信息字上的码元.

(3) 作一个 $n\times r$ Hamming 矩阵 $\boldsymbol{M}_{n\times r}$，将矩阵中第 i 行的行数 i 表示成二进制数$(i)_2$ 后作为该行上的元素，如 $r=2,3,4$ 时，相应的 Hamming 矩阵是

$$\boldsymbol{M}_{3\times2}=\begin{bmatrix}0&1\\1&0\\1&1\end{bmatrix},\boldsymbol{M}_{7\times3}=\begin{bmatrix}0&0&1\\0&1&0\\0&1&1\\1&0&0\\1&0&1\\1&1&0\\1&1&1\end{bmatrix},\boldsymbol{M}_{15\times4}=\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&0&1&1\\0&1&0&0\\0&1&0&1\\0&1&1&0\\0&1&1&1\\1&0&0&0\\1&0&0&1\\1&0&1&0\\1&0&1&1\\1&1&0&0\\1&1&0&1\\1&1&1&0\\1&1&1&1\end{bmatrix}.$$

例如在 $\boldsymbol{M}_{7\times3}$ 中，当第 3 行的行数 3 表示成$(3)_2=011$ 后就把

$\boldsymbol{M}_{7\times 3}$ 中的第 3 行的元素写成 011.

(4) 作矩阵方程 $\boldsymbol{bM}_{n\times r}=\boldsymbol{0}$,展开后即得一个包含 r 个线性方程式的方程组,它的每个方程是一个 b_{2^i} 用 $\boldsymbol{b}$ 中的其余码元表出的等式. 如当 $r=3$ 时的方程组[①]是

$$\begin{cases} b_4+b_5+b_6+b_7=0, \\ b_2+b_3+b_6+b_7=0, \\ b_1+b_3+b_5+b_7=0. \end{cases}$$

(5) 解上面的方程组,得到码元 b_{2^i} $(i=0,1,\cdots,r-1)$,按(2)将它们作为校验位而将信息字的码元放入其余的 m 个空位,即得相应的码字 $\boldsymbol{b}$.

算法 14.12.42 Hamming 码的破译法 与定理 14.12.25 的方法相应,可以利用 $\boldsymbol{bM}=\boldsymbol{0}$ 译码. 设接收字 $\boldsymbol{r}=\boldsymbol{c}\oplus\boldsymbol{e}_i$,这里 $\boldsymbol{c}$ 是码字,而 $\boldsymbol{e}_i$ 是第 i 位为 1 的错误模式. 因 $\boldsymbol{cM}=\boldsymbol{0}$,故 $(\boldsymbol{c}\oplus\boldsymbol{e}_i)\boldsymbol{M}=\boldsymbol{cM}\oplus\boldsymbol{e}_i\boldsymbol{M}=\boldsymbol{0}\oplus\boldsymbol{e}_i\boldsymbol{M}=\boldsymbol{e}_i\boldsymbol{M}$. 因而此乘积其实是错误模式与 $\boldsymbol{M}$ 的乘积. 若此积为零矩阵,则表示传送时未出错,因而接收字即为所求的码字,若此结果为非零矩阵,则此非零矩阵必为矩阵 $\boldsymbol{M}$ 的第 i 行,表示接收字的第 i 位上出错,纠错后即得所求的码字.

定义 14.12.43 若一个 (n,m) 分组码恰能纠正所有重 $\leqslant t$ 的错误模式,则称它为**完全纠 t-错码**(perfect t-errer-correcting code).

定理 14.12.44 Hamming 码是完全纠单错码.

例 14.12.45 求作与 $r=3$ 相应的 Hamming 码,这是(7,4)分组码,原来的信息字集 $\boldsymbol{M}=\{0000,0001,0010,0011,0100,0101,0110,0111,1000,1001,1010,1011,1100,1101,1110,1111\}$. 其 Hamming 矩阵为

---

① 方程组中码元间的加法是"对位布尔和".

$$
\boldsymbol{M}_{7\times 3}=\begin{bmatrix}0&0&1\\0&1&0\\0&1&1\\1&0&0\\1&0&1\\1&1&0\\1&1&1\end{bmatrix}.
$$

设码字为 $\boldsymbol{b}=b_1b_2b_3b_4b_5b_6b_7$，则与它相应的 Hamming 方程 $\boldsymbol{bM}_{7\times 3}=\boldsymbol{0}$，展开得①：

$$
\begin{cases}b_4+b_5+b_6+b_7=0,\\ b_2+b_3+b_6+b_7=0,\\ b_1+b_3+b_5+b_7=0,\end{cases}\quad \text{或} \quad \begin{cases}b_4=b_5+b_6+b_7,\\ b_2=b_3+b_6+b_7,\\ b_1=b_3+b_5+b_7.\end{cases}
$$

用信息字上的码元代入方程组算出 b_4,b_2,b_1 值作为校验位，然后加入相应的信息位即得所求的码：

$0000\mapsto 0000000$，　$0001\mapsto 1101001$，

$0010\mapsto 0101010$，　$0011\mapsto 1000011$，

$0100\mapsto 1001100$，　$0101\mapsto 0100101$，

$0110\mapsto 1100110$，　$0111\mapsto 0001111$，

$1000\mapsto 1110000$，　$1001\mapsto 0011001$，

$1010\mapsto 1011010$，　$1011\mapsto 0110011$，

$1100\mapsto 0111100$，　$1101\mapsto 1010101$，

$1110\mapsto 0010110$，　$1111\mapsto 1111111$.

下面再看在这个码中如何检单错和纠单错. 从码 $\boldsymbol{c}$ 中取码字 $\boldsymbol{b}=0001111$，使它与 $\boldsymbol{M}_{7\times 3}$ 相乘可得 $\boldsymbol{bM}=000$，所以这个码字是正

---

① 方程组码元间的加法是“对位布尔和”.

确的,但若在传送中某位(假设是第 3 位)出错,变成 $\boldsymbol{r}=\boldsymbol{b}\oplus\boldsymbol{e}_3=$ 0011111,则 $\boldsymbol{r}\cdot\boldsymbol{M}_{7\times3}=(\boldsymbol{b}\oplus\boldsymbol{e}_3)\boldsymbol{M}_{7\times3}=011$,它恰是 $\boldsymbol{M}_{7\times3}$ 的第 3 行,且 011 恰是第 3 行的行号"3"的二进制数,因此将 $\boldsymbol{r}$ 的第 3 个码元改正后即得正确的码字 0001111,取出其第 3,5,6,7 位上的码元即可恢复原来的信息字是 0111.

15 环与域

环是有两个二元运算的代数结构，由于附加条件不同，可有各种环，如交换环、有单元的环、整环、除环、域等等. 环的内容较之群论更为丰富，关系更为复杂，但在研究方法及所得结果方面却常与群论平行，因此群论可作为研究环及其他结构的借鉴.

15.1 定义、例子及简单性质

定义 15.1.1 具有两个二元运算"+"与"·"的集 R 所构成的代数结构 $\langle R;+,\cdot\rangle$ 若满足以下三个条件，则称为**环**(ring)：

(1) $\langle R;+\rangle$ 是交换群(或加群)；

(2) $\langle R;\cdot\rangle$ 是半群①(或乘法半群)

(3) 在 $\langle R;+,\cdot\rangle$ 中(左、右)分配律成立，即 $\forall a,b,c\in R$,

$a\cdot(b+c)=a\cdot b+a\cdot c,(b+c)\cdot a=b\cdot a+c\cdot a.$

例 15.1.2 (1) 整数集 $\mathbf{Z}$，有理数集 $\mathbf{Q}$，实数集 $\mathbf{R}$，复数集 $\mathbf{C}$，实数集的子集 $\mathbf{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$ 以及 Gauss 整数集 $\mathbf{Z}(\mathrm{i})=\{m+n\mathrm{i}\mid m,n\in\mathbf{Z}\}$ 关于数的加法"+"与乘法"·"各构成环 $\langle\mathbf{Z};+,\cdot\rangle$，$\langle\mathbf{Q};+,\cdot\rangle$，$\langle\mathbf{R};+,\cdot\rangle$，$\langle\mathbf{C};+,\cdot\rangle$，$\langle\mathbf{Q}(\sqrt{2});+,\cdot\rangle$ 以及 $\langle\mathbf{Z}(\mathrm{i});+,\cdot\rangle$.

(2) 在闭区间[0,1]上的实值连续函数集 Γ 关于函数的加法

---

① 有些作者亦有要求 $\langle R;\cdot\rangle$ 是一个单元半群的，为了使环的外延尽可能宽一些并使其划分更细一些，这里采用的是 Van der Waerden 所著的 Algebra 及 N. Jacobson 所著的 Lectures In Abstract Algebra 上的定义.

与乘法：

$$(f+g)(x)=f(x)+g(x),(f\cdot g)(x)=f(x)g(x).$$

构成实值连续函数环$\langle\Gamma;+,\cdot\rangle$.

(3) 二元集 $B_2=\{0,1\}$关于对位布尔和$\oplus$及布尔积 · 构成(见表 15.1)布尔环$\langle B_2;\oplus,\cdot\rangle$.

表 15.1

$\oplus$	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

(4) 偶数集 $E=\{2n\mid n\in\mathbf{Z}\}$关于数的加法和乘法构成环，称为偶数环.

(5) 设 n 是一个自然数，$\mathbf{Z}_n$ 是模 n 同余类集(例 14.2.7)$\mathbf{Z}_n=\{C_0,C_1,\cdots,C_{n-1}\}$. 其中 $C_k=\{tn+k\mid t\in\mathbf{Z},0\leqslant k<n\}$，同余类的加法"+"和乘法"·"分别是

$$C_i+C_j=C_{i+j},C_i\cdot C_j=C_{i\cdot j},$$

则可证$\langle\mathbf{Z}_n;+,\cdot\rangle$是环，称为模 n 的同余类环.

定理 15.1.3 在环$\langle R;+,\cdot\rangle$中以下各计算法则成立：对于$\forall a,b,a_1,\cdots,a_m,b_1\cdots,b_n\in R$，有

(1) $-(a+b)=(-a)+(-b)$,

(2) 设 $m,n\in\mathbf{Z}$，则

$$n(a+b)=na+nb,$$
$$(m+n)a=ma+na,$$
$$(mn)a=m(na).$$

(3) $(a_1+a_2+\cdots+a_m)\cdot(b_1+b_2+\cdots+b_n)=a_1\cdot b_1+a_1\cdot b_2+\cdots+a_1\cdot b_n+a_2\cdot b_1+a_2\cdot b_2+\cdots+a_2\cdot b_n+\cdots+a_m\cdot b_1+a_m\cdot b_2+\cdots+a_m\cdot b_n$,

或 $$(\sum_{i=1}^{m}a_i)\cdot(\sum_{j=1}^{n}b_j)=\sum_{i\cdot j=1}^{m\cdot n}a_i\cdot b_j.$$

(4) $a\cdot 0=0\cdot a=0$.

(5) $(-a)\cdot b=-a\cdot b=a\cdot(-b)$.

(6) $(-a)\cdot(-b)=a\cdot b$.

由定理 15.1.3(4)可知,环中的两个元 a 与 b 若有一个是零元素,则其乘积 $a\cdot b$ 也是零元素.但在环里由 $a\cdot b=0$ 却未必能推出 $a=0$ 或 $b=0$,这由例 15.1.2 中就可看出:在闭区间[0,1]上的实值连续函数环$\langle\Gamma;+,\cdot\rangle$中,定义函数

$$f(x)=\begin{cases}0 & \left(0\leqslant x\leqslant\frac{1}{2}\right),\\ x-\frac{1}{2} & \left(\frac{1}{2}<x\leqslant 1\right);\end{cases}$$

$$g(x)=\begin{cases}-x+\frac{1}{2} & \left(0\leqslant x\leqslant\frac{1}{2}\right),\\ 0 & \left(\frac{1}{2}<x\leqslant 1\right).\end{cases}$$

则 $f\neq 0$ 且 $g\neq 0$,但 $f\cdot g=0$.

类似地,在模 n 同余类环 Z_n 中,若 n 不是素数,设 $n=ab$,则 $n+a,n+b$. 所以 $C_a\neq C_0$ 及 $C_b\neq C_0$,但

$$C_a\cdot C_b=C_{ab}=C_n=C_0.$$

定义 15.1.4 若在环 R 里,$a,b\in R$,且 $a\neq 0,b\neq 0$,但 $a\cdot b=0$,则称 a 是该环的**左零因子**(left zero divisor),b 是该环的**右零因子**(right zero divisor).

一个环有无零因子与消去律是否成立有密切的关系.

定理 15.1.5 在一个没有零因子的环(称为整环),(见定义 15.1.6(3))中左、右消去律都成立,即

左消去律:$a\neq 0,a\cdot b=a\cdot c\Rightarrow b=c$;

右消去律:$a\neq 0,b\cdot a=c\cdot a\Rightarrow b=c$.

反之,在一个环里若有一个消去律成立,则这个环没有零因子,因而另一个消去律也自动成立.

下面对环进行初步的分类.

定义 15.1.6 (1) 若环$\langle R;+,\cdot\rangle$的乘法半群是可交换的,则称它为**交换环**(commutative ring).

(2) 若环$\langle R;+,\cdot\rangle$的乘法半群是单元半群,则称它为**有单元的环**(ring with unity element),并称它的乘法单元为环的单元.

(3) 若环$\langle R;+,\cdot\rangle$不含零因子,则称为**整环**[①](integral domain).

(4) 若环$\langle R;+,\cdot\rangle$至少有两个以上的元素,而且它的非零元素的集合R^*构成乘法半群的一个子群$\langle R^*;\cdot\rangle$,则称它为**除环**(division ring).

(5) 可交换除环称为**域**(field).

例 15.1.7 (1) 例 15.1.2 中的 6 个数环$\langle \mathbf{Z};+,\cdot\rangle$,$\langle \mathbf{Q};+,\cdot\rangle$,$\langle \mathbf{R};+,\cdot\rangle$,$\langle \mathbf{C};+,\cdot\rangle$,$\langle \mathbf{Q}(\sqrt{2});+,\cdot\rangle$以及$\langle \mathbf{Z}(\mathrm{i});+,\cdot\rangle$都是有单元(数 1)、无零因子的交换环.因而也是整环,其中$\langle \mathbf{Q};+,\cdot\rangle$,$\langle \mathbf{R};+,\cdot\rangle$,$\langle \mathbf{C};+,\cdot\rangle$,$\langle \mathbf{Q}(\sqrt{2});+,\cdot\rangle$是域,因为它们的非零元素的集分别构成其乘法半群的子群.

(2) 环$\langle B_2;+,\cdot\rangle$(见例 15.1.2)构成一个域.

(3) 偶数环$\langle E;+,\cdot\rangle$(见例 15.1.2)是一个无零因子的交换环,所以是一个整环,但它没有单元.

(4) $[0,1]$上的实值连续函数环$\langle \mathbf{\Gamma};+,\cdot\rangle$(见例 15.1.2)是有单元 1(恒等于 1 的函数)的交换环,因它有零因子,故不是整环.

(5) 模 n 同余类环$\langle \mathbf{Z}_n;+,\cdot\rangle$是有单元 C_1 的交换环.当 n 为

---

① 有些作者将整环定义为有单元、无零因子的交换环.另一些则将它定义为无零因子的交换环.

合数时，它有零因子，所以不是整环；但当 n 为素数 p 时，可以证明它的每个非零元素都有逆元素，因而其非零元素的集构成它的乘法半群的子群，所以此时 $\langle \mathbf{Z}_p;+,\cdot\rangle$ 是一个域.

定理 15.1.8 在交换环 $\langle R;+,\cdot\rangle$ 中，二项式定理成立，即若 $\forall a,b\in R, n\in\mathbf{N}$，则

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + b^n,$$

其中

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

定理 15.1.9 (1) 在一个除环 $\langle R;+,\cdot\rangle$ 中，设 $a,b\in R$，则方程 $a\cdot x=b$ 及 $y\cdot a=b$ 各有唯一解：

$$x=a^{-1}\cdot b \text{ 及 } y=b\cdot a^{-1}.$$

(2) 在域 $\langle F;+,\cdot\rangle$ 中，方程 $a\cdot x=b$ 及 $x\cdot a=b$ $(a,b\in F)$ 的唯一解都是 $x=a^{-1}\cdot b$.

15.2 特殊环

上节所述环都是由数集和函数集构成的，它们都是交换环，本节将介绍两个重要的非交换环.

15.2.1 *n* 阶全方阵环

设 R 是环，用 R 中的元素可构成一个 $n\times n$ 矩阵(或 n 阶方阵)：

$$(a_{ij}) = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

所有 n 阶方阵的集合：

$$R_n = \{(a_{ij}) \mid a_{ij}\in\mathbf{R}\}.$$

规定两个方阵相等当且仅当它们对应位置上的元素相等.

定理 15.2.1 环 R 上的所有 n 阶方阵构成的集 R_n 关于矩阵的加法和乘法构成环 $\langle R_n;+,\cdot\rangle$，称它为 R 上的 **n 阶全方阵环**(total matric ring).

定理 15.2.2 若环 R 有单元 1，则 n 阶全方阵环 $\langle R_n;+,\cdot\rangle$ 也有单元(它就是 n 阶单位方阵 $\begin{bmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{bmatrix}$).

定理 15.2.3 设环 R 至少包含一个非零元 a，并且它不是 R 的零因子，则 $\forall n\geqslant 2$，全方阵环 $\langle R_n;+,\cdot\rangle$ 都不是交换环，且都有零因子.

例 15.2.4 如定理 15.2.3，在 R_n 中取两个方阵

$$\boldsymbol{A}=\begin{bmatrix}a & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ & \cdots\cdots\cdots & & \\ 0 & 0 & \cdots & 0\end{bmatrix},\qquad \boldsymbol{B}=\begin{bmatrix}0 & a & \cdots & 0\\ 0 & 0 & \cdots & 0\\ & \cdots\cdots\cdots & & \\ 0 & 0 & \cdots & 0\end{bmatrix},$$

作乘积得

$$\boldsymbol{A}\cdot\boldsymbol{B}=\begin{bmatrix}0 & a^2 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ & \cdots\cdots\cdots & & \\ 0 & 0 & \cdots & 0\end{bmatrix},\qquad \boldsymbol{B}\cdot\boldsymbol{A}=\begin{bmatrix}0 & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ & \cdots\cdots\cdots & & \\ 0 & 0 & \cdots & 0\end{bmatrix}=\boldsymbol{0}.$$

所以 $\boldsymbol{A}\cdot\boldsymbol{B}\neq\boldsymbol{B}\cdot\boldsymbol{A}$.

由 $\boldsymbol{B}\cdot\boldsymbol{A}=0$，知 $\boldsymbol{B}$ 和 $\boldsymbol{A}$ 都是 R_n 的零因子.

15.2.2 四元数除环

设复数对的集 $H=\{(\alpha,\beta)\mid\alpha,\beta\in\mathbf{C}\}$，在其中定义两复数对 (α_1,β_1)，(α_2,β_2) 相等、相加、相乘如下：

$$(\alpha_1,\beta_1)=(\alpha_2,\beta_2)\Leftrightarrow\alpha_1=\alpha_2 \text{ 且 } \beta_1=\beta_2;$$

$$(\alpha_1,\beta_1)+(\alpha_2,\beta_2)=(\alpha_1+\alpha_2,\beta_1+\beta_2);$$

$$(\alpha_1,\beta_1)\cdot(\alpha_2,\beta_2)=(\alpha_1\alpha_2-\beta_1\bar{\beta}_2,\alpha_1\beta_2+\beta_1\bar{\alpha}_2),$$

其中 $\bar{\beta}_2,\bar{\alpha}_2$分别是$\beta_2,\alpha_2$的共轭数.

定理 15.2.5 $\langle H;+,\cdot\rangle$其中 H 是复数对集,是非交换除环,它的每一个非零元$(\alpha,\beta)\neq(0,0)$的逆元是

$$(\alpha,\beta)^{-1}=\left(\frac{\bar{\alpha}}{\alpha\bar{\alpha}+\beta\bar{\beta}},\frac{-\beta}{\alpha\bar{\alpha}+\beta\bar{\beta}}\right).$$

该环称作**四元数除环**(division ring of quaternions),它的元称作**四元数**(quaternion).

它不是交换环,因为

$$(\mathrm{i},0)\cdot(0,1)\neq(0,1)\cdot(\mathrm{i},0).$$

例 15.2.6 四元数的另一种表示法 通过直接验证,任一四元数$(\alpha,\beta)=(a+b\mathrm{i},c+d\mathrm{i})$ $(a,b,c,d\in\mathbf{R})$,都可写成

$$(a,0)\cdot(1,0)+(b,0)\cdot(\mathrm{i},0)+(c,0)\cdot(0,1)+(d,0)\cdot(0,\mathrm{i})$$

的形式,由“同构”的观点,可直接将$(a,0),(b,0),(c,0),(d,0)$取作 a,b,c,d,记$(1,0)=1,(\mathrm{i},0)=\mathrm{i},(0,1)=\mathrm{j},(0,\mathrm{i})=\mathbf{k}$,这样就可将四元数$(a+b\mathrm{i},c+d\mathrm{i})$表示成以下常用形式:

$$a+b\mathrm{i}+c\mathrm{j}+d\mathbf{k}.$$

在 i,j,k 间有以下关系:

$$\mathrm{i}^2=\mathrm{j}^2=\mathrm{k}^2=-1,$$

$$\mathrm{ij}=-\mathrm{ji}=\mathrm{k},\mathrm{jk}=-\mathrm{kj}=\mathrm{i},\mathrm{ki}=-\mathrm{ik}=\mathrm{j}.$$

15.3 子环与中心

定义 15.3.1 设$\langle R;+,\cdot\rangle$是环,S 是 R 的子集,如果$\langle S;+,\cdot\rangle$是环,则称$\langle S;+,\cdot\rangle$为$\langle R;+,\cdot\rangle$的**子环**(subring),简称 S 是环 R 的子环.

类似地可以定义**子除环**(division subring)、**子整环**(integral subdomain)、**子域**(sub field)的概念.

例 15.3.2 (1) R 本身也是环 R 的子环.由零元素构成的单元素集$\{0\}$也是 R 的子环.这两个子环称为 R 的平凡子环.

(2) 在整数整环$\langle \mathbf{Z};+,\cdot\rangle$中,偶数环$\langle E;+,\cdot\rangle$是它的子整环.

(3) 在复数域$\langle \mathbf{C};+,\cdot\rangle$中,实数域 $\mathbf{R}$、有理数域 $\mathbf{Q}$ 都是 $\mathbf{C}$ 的子域(当然也是它的子除环).

定理 15.3.3 (1) 环(整环)R 的非空子集 S 构成子环(子整环)的充要条件是:

$\forall a,b\in S\Rightarrow a-b,a\cdot b\in S.$

(2) 除环(域)R 的子集 S 构成子除环(子域)的充要条件是:

1) S 至少包含一个非零元;

2) $a,b\in S\Rightarrow a-b\in S$;

$a,b\in S,b\neq 0\Rightarrow a\cdot b^{-1}\in S.$

定理 15.3.4 设 $S_1,S_2,\cdots,S_n$都是环 R 的子环,则它们的交集 $S=S_1\cap S_2\cap\cdots\cap S_n$也是 R 的子环.

定理 15.3.5 设 C 是由环 R 中一切可以与 R 的每个元交换的元素 c 所组成的集:

$$C=\{c\mid c\in R,\forall r\in R,c\cdot r=r\cdot c\},$$

则 C 是 R 的一个子环.称为环 R 的**中心**(center).

由于每个环都含有零元素 0,而 $0\cdot r=r\cdot 0=0$,所以每个环都有中心.

特别地,若 R 是有单元 1 的环,显然 $1\in C$;若 R 是交换环,则它的中心 $C=R$.

15.4 理想与商环

定义 15.4.1 设 I 是环 R 的一个非空子集,如果它能满足以下两个条件,则称它为环 R 的**理想**(ideal):

(1) $a,b\in I\Rightarrow a-b\in I$,

(2) $a\in I, r\in R\Rightarrow ra, ar\in I$.

与定理 15.3.3 对比可见：R 的一个理想必是它的一个子环，但 R 的子环未必是它的理想，因为理想所满足的条件要比子环稍强.

例 15.4.2 (1) 在任一环 R 中，$\{0\}$ 及 R 本身都是 R 的平凡理想，前者称为**零理想**(zero ideal)，后者称为**单位理想**(unit ideal).

(2) 在整数环 $\mathbf{Z}$ 中，任取一整数 $n\begin{pmatrix}n\neq 0\\ n\neq 1\end{pmatrix}$，则它的一切倍数所成的集 $I=\{rn\mid r\in\mathbf{Z}\}$ 构成它的理想.

(3) 环 R 上的一元多项式集 $R[x]=\{a_0+a_1x+a_2x^2+\cdots+a_nx^n\mid a_i\in R\}$ 关于多项式的加法与乘法构成一个环，称为环 R 上的多项式环，在这个环里，所有常数项为 0 的多项式集 $I=\{b_1x+b_2x^2+\cdots+b_mx^m\mid b_i\in R, m\geqslant 1\}$ 构成 $R[x]$ 的一个理想.

(4) 除环(或域) R 只能有零理想和单位理想，不可能有其他理想. 这是因为它们的任一非零理想 I 的任一非零元素 a 都是可逆的，因而 $a^{-1}\cdot a=1\in I$，故 R 的每个元素 $b=b\cdot 1\in I$，因此 $I=R$ 是单位理想.

定理 15.4.3 设 $\{I_\alpha\}_{\alpha\in A}$ 是环 R 中的理想族，则 $I=\bigcap\{I_\alpha\mid\alpha\in A\}$ 仍是 R 中的理想.

设 $X\subset R$ 是环 R 中的子集，由定理 15.4.3 知 $J(X)=\bigcap\{I\mid I$ 是 R 中的理想且 $X\subset I\}$ 仍是一个理想，它是 R 中包含集合 X 的最小理想. 特别当 $X=\{a\}$(集合 X 仅由单个元素 a 构成)时，称 J 是由 a 生成的**主理想**(principal ideal)，用 $J=(a)$ 表示.

下面介绍利用环的理想作出与原环有密切关系的新环：设 I 是环 $\langle R;+,\cdot\rangle$ 的一个理想，则 $\langle I;+\rangle$ 是加群 $\langle R;+\rangle$ 的一个正规子群，根据群的分解理论(14.10.1 节) R 被 I 分解成若干个陪集

的族：

$$\pi_I = R/I = \{x + I \mid x \in R\},$$

其中每个陪集 $x+I$ 由一切形如 $x+u(u \in I)$ 的元构成：

$$x + I = \{x + u \mid u \in I\}.$$

在陪集族 R/I 中，规定加法"＋"和乘法"·"如下：

$$(a + I) + (b + I) = (a + b) + I;$$

$$(a + I) \cdot (b + I) = (a \cdot b) + I.$$

则有以下定理.

定理 15.4.4 设 R 是环，I 是它的一个理想，R/I 是 I 的陪集的族，它关于陪集的加法和乘法构成环 $\langle R/I; +, \cdot \rangle$，称它为 R 关于理想 I 的**商环**(quotient ring)或**差环**(difference ring)或**同余类环**(residue class ring).

定理 15.4.5 (1) 设 R 是交换环，I 是它的一个理想，则商环 R/I 也是交换环.

(2) 设 R 是有单元的环，I 是它的理想，则商环 R/I 也有单元，就是 R 的单元 1 所在的陪集 $1+I$.

现在利用以上理论来阐明整数环 $\mathbf{Z}$ 与模 n 同余类环 $\mathbf{Z}_n$（例 15.1.2）之间的关系. 其实 $\mathbf{Z}_n$ 就是 $\mathbf{Z}$ 关于理想 $I=(n)=\{tn \mid t \in \mathbf{Z}\}$ 的商环 $\mathbf{Z}/(n)$，它的两个陪集(模 n 同余类)C_a 与 C_b 相等的充要条件是 $a \equiv b(\bmod n)$.

由例 15.1.7 知模 n 同余类环 $\mathbf{Z}_n$ 当 n 是素数时是域；当 n 是合数时有零因子，但此时 $\mathbf{Z}_n$ 仍可能有可逆元(例如 C_1)，则称它为**单位**[①](unit)，可以证明 $\mathbf{Z}_n$ 的一个同余类 C_a 是一个单位当且仅当 $(a,n)=1$(即 a,n 互素). 因而在 $\mathbf{Z}_n=\{C_0, C_1, C_2, \cdots, C_{n-1}\}$ 中单位的个数是小于等于 n 且与 n 互素的正整数的个数，即 n 的 Euler

---

① 注意"单位"与"单元"的区别，前者指存在逆元 a^{-1} 的元素，a：$a^{-1} \cdot a = a \cdot a^{-1} = e$，因而单元必定是单位，但单位却未必是单元.

函数值 $\varphi(n)$.

定理 15.4.6 同余类环 $\mathbf{Z}_n$ 的所有单位构成的集 $G_u=\{C_a \mid (a,n)=1\}$ 关于同余类乘法构成一个群 $\langle G_u;\cdot\rangle$,它的阶为 $\varphi(n)$.

定理 15.4.7 Euler-Fermat 定理 设整数 a 与正整数 n 互素,则

$$a^{\varphi(n)}\equiv 1(\mathrm{mod}n).$$

当 n 是素数 p 时,$\varphi(p)=p-1$,进而又有下面定理.

定理 15.4.8 若 p 是素数,$a\not\equiv 0(\mathrm{mod}p)$,则

$$a^{p-1}\equiv 1(\mathrm{mod}p).$$

此定理还可作如下的推广.

定理 15.4.9 设 p 是素数,则 $\forall a\in\mathbf{Z}$ 都有

$$a^p\equiv a(\mathrm{mod}p).$$

例 15.4.10 (1) 就 $n=3$ 及 $n=4$ 两种情况考察 $\mathbf{Z}_n$ 的单位所构成的乘群:$\mathbf{Z}_3$ 及 $\mathbf{Z}_4$ 的乘法表如表 15.2.

表 15.2

$\cdot$	C_0	C_1	C_2
C_0	C_0	C_0	C_0
C_1	C_0	C_1	C_2
C_2	C_0	C_2	C_1

$\cdot$	C_0	C_1	C_2	C_3
C_0	C_0	C_0	C_0	C_0
C_1	C_0	C_1	C_2	C_3
C_2	C_0	C_2	C_0	C_2
C_3	C_0	C_3	C_2	C_1

由表 15.2 可见,在 $\mathbf{Z}_3$ 里 C_1,C_2 都是单位,而且 $C_1^{-1}=C_1,C_2^{-1}=C_2$. 所以 $G_u=\{C_1,C_2\}$,它的阶$=\varphi(3)=2$. $\mathbf{Z}_4$ 的 C_1 与 C_3 是单位,其余二元素都不是单位,所以 $G_u=\{C_1,C_3\}$,它的阶$=\varphi(4)=2$.

(2) 在 $n=4$ 的情况下验证 Euler-Fermat 定理:现取 $a=5$,则 4 与 5 是互素的,由于 $\varphi(4)=2$,$5^{\varphi(n)}=5^2=25\equiv 1(\mathrm{mod}4)$,显然成立.

15.5 环的同态、同构与反同构

本节介绍某些特殊环(主要是非交换环)的反同构概念.

定义 15.5.1 设 φ 是环 $\langle R;+,\cdot\rangle$ 到环 $\langle R';+',\cdot'\rangle$ 上的一个映射,如果满足以下条件,则称 φ 为环 R 到环 R' 的**同态映射**(homomorphism mapping).

(1) $\varphi(a+b)=\varphi(a)+'\varphi(b)$;

(2) $\varphi(a\cdot b)=\varphi(a)\cdot'\varphi(b)$.

此时,称环 $\langle R;+,\cdot\rangle$ 与 $\langle R';+',\cdot'\rangle$ **同态**(homomorphism),并用 $R\sim R'$ 表示.

类似地,可给出环的同构、自同构等概念.

定义 15.5.2 如果环 $\langle R;+,\cdot\rangle$ 到环 $\langle R';+',\cdot'\rangle$ 上的一个双射 φ 满足以下条件,则称 φ 为环 R 到 R' 的**反同构**(anti-isomorphism):

(1) $\varphi(a+b)=\varphi(a)+'\varphi(b)$,

(2) $\varphi(a\cdot b)=\varphi(b)\cdot'\varphi(a)$.

例 15.5.3 (1) 在整数环 $\langle \mathbf{Z};+,\cdot\rangle$ 与模 n 同余类环 $\langle \mathbf{Z}_n;+,\cdot\rangle$ 间作映射.

$$\varphi:\quad a\mapsto C_a \qquad (\forall a\in\mathbf{Z}),$$

则 φ 是 $\mathbf{Z}$ 到 $\mathbf{Z}_n$ 的一个同态满射.因而 $\mathbf{Z}\sim\mathbf{Z}_n$.

(2) 在复数域 $\mathbf{C}=\{a+b\mathrm{i}\mid a,b\in\mathbf{R}\}$ 与 $\mathbf{R}$ 上的方阵环 $\boldsymbol{M}_2=\left\{\begin{bmatrix} a & b\\ -b & a\end{bmatrix}\middle| a,b\in\mathbf{R}\right\}$ 间作映射:

$$\varphi:\quad a+b\mathrm{i}\mapsto\begin{bmatrix} a & b\\ -b & a\end{bmatrix},$$

则 φ 是 $\mathbf{C}$ 到 $\boldsymbol{M}_2$ 的同构映射,因而

$$\mathbf{C}\cong\boldsymbol{M}_2.$$

(3) 在复数域 **C** 里，映射

$$\varphi:\quad \alpha=a+b\mathrm{i}\mapsto\bar{\alpha}=a-b\mathrm{i}$$

是 **C** 中的一个自同构.

(4) 在四元数除环 $H=\{a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}\mid a,b,c,d\in\mathbf{R}\}$（见定理 15.2.5 及例 15.2.6）与实数域上的四阶方阵环 $\boldsymbol{M}_4=\left\{\begin{bmatrix} a & b & c & d\\ -b & a & -d & c\\ -c & d & a & -b\\ -d & -c & b & a\end{bmatrix}\middle|\ a,b,c,d\in\mathbf{R}\right\}$间作映射

$$\varphi:\quad a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}\mapsto\begin{bmatrix} a & b & c & d\\ -b & a & -d & c\\ -c & d & a & -b\\ -d & -c & b & a\end{bmatrix},$$

则 φ 是 H 与 $\boldsymbol{M}_4$ 间的一个同构（即四元数的矩阵表示法）.

(5) 设 $\alpha=a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}\in H$，称 $\bar{\alpha}=a-b\mathrm{i}-c\mathrm{j}-d\mathrm{k}$ 为 α 的共轭数，在 H 内作映射：

$$\varphi:\alpha\mapsto\bar{\alpha},$$

则可直接验证

$$\varphi(\alpha+\beta)=\overline{\alpha+\beta}=\bar{\alpha}+\bar{\beta}=\varphi(\alpha)+\varphi(\beta),$$
$$\varphi(\alpha\cdot\beta)=\overline{\alpha\cdot\beta}=\bar{\beta}\cdot\bar{\alpha}=\varphi(\beta)\cdot\varphi(\alpha),$$

所以 φ 是 H 自身的反同构.

(6) 设 R 是交换环，在它上面的 n 阶全方阵环 $R_n=\{(a_{ij})\mid a_{ij}\in R,i,j=1,2,\cdots,n\}$ 中作映射 φ 使 (a_{ij}) 与它的转置方阵 $(a_{ij})^{\mathrm{T}}$ 相对应：

$$\varphi:(a_{ij})\mapsto(a_{ij})^{\mathrm{T}}$$

则因

$$[(a_{ij})+(b_{ij})]^{\mathrm{T}}=(a_{ij})^{\mathrm{T}}+(b_{ij})^{\mathrm{T}},$$
$$[(a_{ij})\cdot(b_{ij})]^{\mathrm{T}}=(b_{ij})^{\mathrm{T}}\cdot(a_{ij})^{\mathrm{T}},$$

及 φ 是 R_n 到自身的双射可知，φ 是 R_n 中的反自同构.

下面介绍同态、同构的作用和性质：

定理 15.5.4 (1) 设 φ 是环 R 到环 R' 的同态，ψ 是环 R' 到环 R'' 的同态，则它们的积 $\psi\cdot\varphi$ 是环 R 到 R'' 的同态.

(2) 设 φ 是环 R 到 R' 的同构，则 φ 的逆映射 φ^{-1} 是 R' 到 R 的同构.

定理 15.5.5 设 R 是环，R' 是有两个代数运算 $+'$，$\cdot'$ 的集，如果存在 R 到 R' 的满射，使得 R 与 R' 同态，则 R' 也是环.

简言之，环的同态像也是环.

定理 15.5.6 设环 $\langle R;+,\cdot\rangle \sim \langle R';+',\cdot'\rangle$，则

(1) R 中零元素的像是 R' 的零元素；

(2) R 中元素 a 的负元的像是 a 的像的负元；

(3) 若 R 是交换环，则 R' 也是交换环；

(4) 如果 R 有单元 1，则 R' 有单元 $1'$，而且 $1'$ 是 1 的像.

注意：两个同态的环有无零因子是互不相干的，换言之：R 无零因子并不能保证它的同态像 R' 无零因子，反之亦然.

定理 15.5.7 在环 R 到环 R' 的同态满射之下，

(1) R 的子环 S 的像 S' 是 R' 的子环；

(2) R 的理想 I 的像 I' 是 R' 的理想；

(3) R' 的子环 S' 的逆像 S 是 R 的子环；

(4) R' 的理想 I' 的逆像 I 是 R 的理想.

换言之，子环及理想经过同态映射后是不变的.

如果把同态换成同构，这种不变性还有更重要的意义.

定理 15.5.8 设环 $R\cong R'$，

(1) 若 R 是整环，则 R' 也是整环；

(2) 若 R 是除环，则 R' 也是除环；

(3) 若 R 是域，则 R' 也是域.

与群类似，环 R 到 R' 的同态满射 φ 的核 $\ker\varphi$ 仍是 R' 的零元 $0'$ 在 φ 之下的所有逆像构成的 R 的子集：

$$\ker\varphi=\{r \mid r\in R, \varphi(r)=0'\}.$$

定理 15.5.9　环的同态基本定理(fundamental theorem of homomorphism)　设 R 是环，I 是它的理想，则 R 必与商环 R/I 同态：

$$R\sim R/I;$$

反之，若 R 及 R' 是两个环，而且 $R\sim R'$，则此同态满射 φ 的核 $\ker\varphi$ 是 R 的理想，而且

$$R/\ker\varphi\cong R'.$$

该定理表明：每个环必定与它的商环且仅能与它的商环同态，因为它的任何同态像都与它的商环同构.

例 15.5.10　设 n 是整数环 $\mathbf{Z}$ 的一个非零整数(元素)，则 n 的一切整倍数构成一个由 n 生成的主理想 $(n)=\{tn \mid t\in\mathbf{Z}\}$. 作商环 $R/(n)$ 得到模 n 同余类环 $\mathbf{Z}_n=\{C_0, C_1, C_2, \cdots, C_{n-1}\}$，这时 $\mathbf{Z}$ 到 $\mathbf{Z}_n$ 的映射

$$\varphi: m\mapsto C_m$$

显然是同态满射，故 $\mathbf{Z}\sim\mathbf{Z}_n$. 这就验证了同态定理的第一部分.

验证第二部分：设 $R\sim R'$，若此时的同态满射是 φ，则可证 $I=\ker\varphi$ 是 R 的一个理想. 作商环 $R/I=\{a+I, b+I, \cdots\}$，这里的 $a, b, \cdots\in R$，$a+I, b+I, \cdots$ 表示元素 $a, b, \cdots$ 所在的陪集，今在 R/I 与 R' 间作映射

$$\psi: r+I\mapsto r'=\varphi(r)\quad(r\in R),$$

则可证 ψ 是 R/I 到 R' 的同构映射

$$R/I\cong R'.$$

15.6　环的特征

初等代数中绝大部分数的运算法则在一般环中都适用，但在某些环中有些法则未必适用，如乘法交换律以及由它派生的一些

法则在非交换环中未必适用，消去律在有零因子的环中也不适用。从下面的例子还可看到，即使在具有最强条件的域中，非零元素的整倍数必不为零元素这个法则也未必成立。

例 15.6.1 设 p 是素数，则同余类环 $\mathbf{Z}_p$ 是一个域（例 15.1.7）。任取 $C_i \in \mathbf{Z}_p$，作它的 p 倍元素：

$$pC_i = \underbrace{C_i + C_i + \cdots + C_i}_{p\text{个}} = C_{\underbrace{i+i+\cdots+i}_{p\text{个}}} = C_{pi} = C_0$$

这个式子表明 $\mathbf{Z}_p$ 的任意元素（无论是零元素或非零元素）的 p 倍必定为零元素。

产生以上现象的原因是与环 $\langle R; +, \cdot \rangle$ 中加群 $\langle R; + \rangle$ 元素的阶（定义 14.7.9）有关：R 中的元素 a 在加群中的阶若是无限大，则不管 m 是怎样的非零整数，总有 $ma \neq 0$；若 a 的阶是一个有限整数 r，则 $ra=0$。换言之，对于环 R 的非零元素 a 来说，其倍元能否为零元素完全由 a 在加群中的阶是无限或有限而决定。此种情况相当复杂，在某些环里可能某些非零元素的阶是无限的，而另一些却是有限的。为了得到较好结果，今后仅讨论无零因子的环。

定理 15.6.2 在无零因子的环 R 中，所有非零元素在加群中的阶都是相同的，它们或者是无限大，或者同是一个有限整数。

定义 15.6.3 无零因子环 R 的非零元素在其加群中的阶称为**环 R 的特征**(characteristic of ring)。

定理 15.6.4 如果无零因子环 R 的特征是有限整数 n，则 n 是一个素数。

定理 15.6.5 (1) 无零因子环 R 的特征若是无限大，则对于 $\forall a \in R, a \neq 0$ 必有

$$\forall m (\neq 0) \in \mathbf{Z}, ma \neq 0.$$

(2) 无零因子环 R 的特征若是素数 p，则(1)的结论不成立，但有以下公式：

$$(a+b)^p = a^p + b^p.$$

例 15.6.6 (1) 例 15.1.2 的各个数环与数域都是无零因子环，它们的特征都是无限大.

(2) 布尔环 $\langle B_2;+,\cdot\rangle$(例 15.1.2)是一个域，它的特征是 2.

(3) 以素数 p 为模的同余类环 $\mathbf{Z}_p$ 是一个域(例 15.1.7)，它的特征是 p.

15.7 利用最大理想造域

定义 15.7.1 环 R 的非零理想 I，若除 R 及它自身外，不被其他理想包含，则称 I 为**最大理想**(maximal ideal).

定理 15.7.2 设 R 是有单元的交换环. 若 I 是 R 的最大理想，则商环 R/I 是一个域；反之，若商环 R/I 是一个域，则 I 必是 R 的最大理想.

例 15.7.3 在整数环 $\mathbf{Z}$ 中，由一个素数 p 生成的主理想 $I=(p)$ 是一个最大理想. 作商环 R/I，由例 15.1.7 知它就是模 p 同余类环 $\mathbf{Z}_p$，又因 p 为素数，所以它是一个域.

为了说明条件是必要的，设 n 是合数 $n=i\cdot j(1<i,j<n)$，则 n 及 i 生成的主理想分别是 $(n)=\{tn\mid t\in\mathbf{Z}\}$ 及 $(i)=\{t'i\mid t'\in\mathbf{Z}\}$，将二者进行比较即知，$(n)\subset(i)$，故 (n) 不是最大理想，此时 $R/(n)=\mathbf{Z}_n=\{C_0,C_1,\cdots,C_{n-1}\}$ 显然有零因子 C_i 及 C_j，所以 $R/(n)$ 不是域.

15.8 环的嵌入

从本节起将讨论环及域的扩张问题. 因为在一个固定的环中有时常缺乏解决某类问题所必需的性质，例如在整数环中就不能保证整系数方程 $ax=b(a\neq 0)$ 有解. 由于人们创造了有理数域才

解决了这个问题. 类似地,求解有理系数方程 $x^2=2, x^2+1=0$ 等都需要将环与域加以扩张,在进行扩张时,主要使用嵌入和添加两种方法,介绍如下.

定义 15.8.1 设 S 是环,如果它与环 R 的一个子环同构,则称 S 被**嵌入**(imbedding)R 中,称环 R 为 S 的一个**扩张**(extension).

定理 15.8.2 任意环 S 均可被嵌入于有单元的环 R 之中,因此任意环 S 均可扩张成为有单元的环.

15.9 分式域

有理数域是由整数环扩张而成的,本节将仿效这种方法建立某些特殊环的扩域.

定理 15.9.1 每一个非零交换整环 R 都可嵌入一个域 Q 之中.

证明大意:利用 R 的元 $a, b, c, \cdots$ 作集 $A=\left\{\frac{a}{b} \middle| a, b \in R, b \neq 0\right\}$. 并在 A 的元素间定义关系"$\sim$"如下:

$$\frac{a}{b} \sim \frac{a'}{b'} \Leftrightarrow a \cdot b' = a' \cdot b,$$

则可证"$\sim$"是等价关系. 该等价关系把集划分成若干块$\left[\frac{a}{b}\right]$,作这些块的集 $Q_0=\left\{\left[\frac{a}{b}\right] \middle| \frac{a}{b} \in A\right\}$,并规定 Q_0 的加法"$+$"和乘法"$\cdot$"为:

$$\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]=\left[\frac{ad+bc}{bd}\right],$$

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right]=\left[\frac{ac}{bd}\right].$$

可证$\langle Q_0;+,\cdot\rangle$是域,其子集 $R_0=\left\{\frac{qa}{q} \middle| q, a \in R, q \neq 0\right\}$关于

"+"、"·"构成的环与环 R 同构：$R \cong R_0$（只要在 R 与 R_0 间作映射 $\varphi: a \mapsto \frac{qa}{q}$ 就可证 φ 是一个同构映射），由定义 15.8.1 知此环 R 可嵌入于域 Q_0 之中.

利用 $R \cong R_0$ 还可将 Q_0 的构造简化如下：

定理 15.9.2 Q_0 恰好是由所有元 $\frac{a}{b}(a,b \in R, b \neq 0)$ 构成的.

定义 15.9.3 若域 Q 包含环 R，而且 Q 恰是由所有元 $\frac{a}{b}(a,b \in R, b \neq 0)$ 构成的. 则域 Q 称为环 R 的**分式域**(field of fraction)或**商域**(quotient field).

在环 R 的分式域存在时，有以下定理.

定理 15.9.4 (1) 环 R 的分式域 Q 是 R 的最小扩域. 换言之，环 R 的任何扩域 F 均包含 R 的分式域.

(2) 同构环的分式域必同构，因而环的分式域是唯一的.

定理 15.9.5 整数环 $\mathbf{Z}$ 的分式域是有理数域 $\mathbf{Q}$，它是由所有分数 $\frac{a}{b}$ 构成的，且是包含 $\mathbf{Z}$ 的最小扩域. 换言之：任何数域均包含有理数域.

15.10 多项式环

多项式是数学中最常用的工具，本节要建立它的形式理论以阐明其存在性及构造.

定义 15.10.1 设 R_0 是一个有单元 1 的交换环，R 是其子环，并且 $1 \in R$，$\alpha \in R_0$，形如

$a_0 + a_1\alpha + \cdots + a_n\alpha^n \quad (a_i \in R, n$ 是非负整数).

的 R_0 的元素叫做 R 上 α 的**多项式**(polynomial)，a_i 称作多项式的**系数**(coefficient).

定理 15.10.2 环 R 上的 α 多项式的集合

$R[\alpha]=\{a_0+a_1\alpha+\cdots+a_n\alpha^n \mid a_i\in R, n$ 是非负整数$\}$

关于以下定义的加法"+"和乘"·"法构成环$\langle R[\alpha];+,\cdot\rangle$：

$$(a_0+a_1\alpha+\cdots+a_m\alpha^m)+(b_0+b_1\alpha+\cdots+b_n\alpha^n)$$
$$=(a_0+b_0)+(a_1+b_1)\alpha+\cdots+(a_m+b_m)\alpha^m$$
$$+(b_{m+1}+0)\alpha^{m+1}+\cdots+(b_n+0)\alpha^n \quad (m<n),$$
$$(a_0+a_1\alpha+\cdots+a_m\alpha^m)\cdot(b_0+b_1\alpha+\cdots+b_n\alpha^n)$$
$$=c_0+c_1\alpha+\cdots+c_{m+n}\alpha^{m+n}.$$

其中 $$c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0=\sum_{i+j=k}a_ib_j\ .$$

定义 15.10.3 环$\langle R[\alpha];+,\cdot\rangle$称作 R 上的**多项式环**(polynomial ring).

定义 15.10.4 设环 $R_0\supset R$，若 R_0 中元素 x 的任何系数不全为零的多项式都不等于零：

$$a_0+a_1x+\cdots+a_nx^n\neq 0,$$

则 x 称作 R 上的**超越元素**(transcendental element)，否则称为**代数元素**(algebraic element).

例 15.10.5 (1) 对于整数环 **Z** 及有理数域 **Q** 来说，超越数 e 及 π 都是 **Z** 及 **Q** 上的超越元素，因为把它们代入任何非零整系数或非零有理数系数多项式时都不为零，它们仅在代入系数全为零的多项式时才为零.

(2) $\sqrt{2}$ 不是整数环 **Z**、也不是有理数域 **Q**、更不是实数域 **R** 的超越元素，而是它们上的代数元素. 因为它满足整系数(当然也是有理系数)多项式 x^2-2 及实系数多项式 $x-\sqrt{2}$.

(3) 元素 x 是否是 R 上的超越元素与 R 本身的构造密切相关：上面举出的 e 与 π 固然是整数环及有理数域上的超越元素，但对于实数域却不是了，因为它们分别满足实系数多项式 $x-\mathrm{e}$ 及 $x-\pi$.

(4) 对于固定的环 R_0,未必含有 R 上的超越元素,如令 $R=\mathbf{Z}$,R_0 是 Gauss 整数环 $R_0=\{a+b\mathrm{i}\mid a,b\in\mathbf{Z}\}$,对于 $\forall\,\alpha=a+b\mathrm{i}\neq 0\in R_0$,都有

$$(a^2+b^2)+(-2a)\alpha+\alpha^2=0,$$

这就是说,R_0 的任一元素 α 都满足一个非零整系数方程,故 R_0 内不存在 $R(=\mathbf{Z})$ 上的超越元素.

如果不限定扩环则有以下定理.

定理 15.10.6 给定具有单元 1 的交换环 R,必有 R 上的超越元素 x 存在,因而也存在 R 上的多项式环 $R[x]$.

定义 15.10.7 按照陆续添加的方法在环 R 上作出的多项式环 $(\cdots((R[\alpha_1])[\alpha_2])\cdots[\alpha_n])$ 称做 R 上的 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的**多项式环**(polynomial ring). 简记为 $R[\alpha_1,\alpha_2,\cdots,\alpha_n]$. 它包括所有可以写成

$$\sum_{i_1\cdots i_n}a_{i_1\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}\ (a_{i_1i_2\cdots i_n}\in R,\text{但只有有限个 } a_{i_1i_2\cdots i_n}\neq 0)$$

形式的元素,其加法"+"和乘法"·"是

$$\sum_{i_1\cdots i_n}a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}+\sum_{i_1\cdots i_n}b_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}$$
$$=\sum_{i_1\cdots i_n}(a_{i_1\cdots i_n}+b_{i_1\cdots i_n})\alpha_1^{i_1}\cdots\alpha_n^{i_n};$$

$$\Big(\sum_{i_1\cdots i_n}a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}\Big)\cdot\Big(\sum_{j_1\cdots j_n}b_{j_1\cdots j_n}\alpha_1^{j_1}\cdots\alpha_n^{j_n}\Big)$$
$$=\sum_{k_1\cdots k_n}c_{k_1\cdots k_n}\alpha_1^{k_1}\cdots\alpha_n^{k_n},$$

其中 $$c_{k_1\cdots k_n}=\sum_{i_m+j_m=k_m}a_{i_1\cdots i_n}b_{j_1\cdots j_n}\ (m=1,2,\cdots,n).$$

同前可以推广超越元素的概念.

定义 15.10.8 设 $x_1,x_2,\cdots,x_n$ 是环 R_0 的 n 个元,R 是 R_0 的子环,若 R 上的 $x_1,x_2,\cdots,x_n$ 的任何系数不全为 0 的多项式都不等于零,则 $x_1,x_2,\cdots,x_n$ 就叫做 R 上的**独立超越元素**(independent

transcendental element).

定理 15.10.9 给定有单元 1 的交换环 R 及正整数 n 后，必定存在 R 上的独立超越元素 $x_1, x_2, \cdots, x_n$，因而也就存在 R 上的多元多项式环 $R[x_1, x_2, \cdots, x_n]$.

定理 15.10.6 及定理 15.10.9 已回答了多项式环的存在问题，下面考虑它的构造及数量问题.

定理 15.10.10 设 $R_1[x]$是超越元素 x 的多项式环，$R_2[\alpha]$是任意元素 α 的多项式环，σ 是 R_1 到 R_2 的一个同态，则 σ 恰有一种方法扩张成为 $R_1[x]$到 $R_2[\alpha]$上的同态 σ' 使 $\sigma' x=\alpha$.

定理 15.10.11 (1) 若 x 及 y 都是环 R 上的超越元素，则 $R[x]$必与 $R[y]$同构.（换言之，一个环的单个超越元素多项式环是唯一的.）

(2) 若 α 是环 R 上的代数元素，则 $R[\alpha]$必同构于商环 $R[x]/I$，其中 x 是 R 上的超越元素，而 I 是同态映射 $\varphi: R[x]\to R[\alpha]$的核 $\ker\varphi$.

例 15.10.12 试考察 $\mathbf{Q}[\sqrt{2}]$的构造：作 $\mathbf{Q}[x]=\{a_0+a_1x+\cdots+a_nx^n \mid a_i\in\mathbf{Q}, n\in\mathbf{Z}^+\}$到 $\mathbf{Q}[\sqrt{2}]$的映射

$$\varphi: a_0+a_1x+\cdots+a_nx^n \mapsto a_0+a\sqrt{2}+\cdots+a_n(\sqrt{2})^n,$$

则可证

$$\mathbf{Q}[x]\sim\mathbf{Q}[\sqrt{2}].$$

设 $f(x)\in\ker\varphi$，则 $f(\sqrt{2})=0$ 及 $f(-\sqrt{2})=0$（有理系数多项式性质），故 x^2-2 是 $f(x)$的一个因子；反之，若 $f(x)$有一个因子 x^2-2，则 $f(\sqrt{2})=0$，因而 $f(x)\in\ker\varphi$. 所以 $\ker\varphi=\{(x^2-2)t(x) \mid t(x)\in\mathbf{Q}[x]\}=$ 元素 x^2-2 生成的主理想 (x^2-2)（定理 15.4.3），由定理 15.5.9 知存在同构映射 φ，使

$$\mathbf{Q}[x]/(x^2-2)\cong\mathbf{Q}[\sqrt{2}].$$

进一步具体考察 $\mathbf{Q}[\sqrt{2}]$的构造及同构映射 φ. 由于

$$a_0+a_1\sqrt{2}+a_2(\sqrt{2})^2+\cdots+a_n(\sqrt{2})^n=(a_0+2a_2+4a_4+\cdots)+\sqrt{2}(a_1+2a_3+4a_5+\cdots)\in\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}.$$

显然 $$\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}\subseteq\mathbf{Q}[\sqrt{2}],$$

所以 $$\mathbf{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}.$$

由于 $\mathbf{Q}[x]/(x^2-2)=\{[a+bx]\mid a\cdot b\in\mathbf{Q}\}$，这里记号 $[a+bx]$ 表示 $a+bx$ 所在的陪集，故存在于 $\mathbf{Q}[x]/(x^2-2)$ 与 $\mathbf{Q}[\sqrt{2}]$ 间的同构映射 φ 是：

$$\varphi:\quad [a+bx]\mapsto a+b\sqrt{2}.$$

可简写成 $$\varphi:\quad a+bx\mapsto a+b\sqrt{2}.$$

15.11 域的单扩张

域是一种特殊的环，在环上作扩环特别是作多项式环的方法启示我们利用添加的方法可做域的扩张. 各种数的发展过程也是一样，例如实数域是在它的子域有理数域上添加无理数建立起来的，而复数域则是在实数域上添加 $x^2+1=0$ 的根建立起来的. 根据在域上作不同的"添加"而得到各种域，本节将介绍单扩域、代数扩域、多项式的分裂域、有限域和可离扩域等.

定义 15.11.1 若域 F 是域 E 的子域，则 E 称为 F 的**扩域**(extension field).

为了找寻构作扩域的起点，首先要找出最小的域. 在定理 15.9.5 中早已看到有理数域是最小的数域，任何数域都包含有理数域.

定理 15.11.2 设 E 是域，若 E 的特征是 ∞，则 E 含有与有理数域同构的子域；若 E 的特征是素数 p，则 E 含有与模 p 同余

类域 $\mathbf{Z}_p=\mathbf{Z}/(p)$同构的子域.

定义 15.11.3 若域 F 不包含真子域，则称它为**素域**(prime field). 定理 15.11.2 可改述如下.

定理 15.11.4 设 E 是域. 若其特征是∞，则它包含与有理数域同构的素域；若其特征是素数 p，则它包含与 $\mathbf{Z}_p$同构的素域.

定义 15.11.5 添加元素 α 于域 F 所得的扩域称为域 F 的一个**单扩张(或单扩域)**(simple extension)，记作 $F(\alpha)$.

例 15.11.6 $\mathbf{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$是在有理数域 $\mathbf{Q}$ 上添加无理数$\sqrt{2}$所得的单扩域；复数域 $\mathbf{C}=\{a+b\mathrm{i}\mid a,b\in\mathbf{R},\mathrm{i}^2=-1\}$是在实数域 $\mathbf{R}$ 上添加纯虚数 i 的单扩域.

每个域都可由它的素域出发，经过有限或无限的扩张得到；此外，有些域(如有限域，可离扩域)本身就是单扩域，它只需在素域上添加一个元素就可得到.

与定义 15.10.4 中定义环 R 上的超越元素、代数元素一样，在构作域的单扩张时也可以根据所添加的元素是超越元素或代数元素而分成**单超越扩域**(simple transcendental extension)及**单代数扩域**(simple algebraic extension)两种，它们的构造有明显的区别，可从以下两个定理看到.

定理 15.11.7 若 α 是域 F 上的超越元素，则 $F(\alpha)\cong F[x]$的分式域.

这里 $F[x]$是添加了 F 上的一个超越元素 x 后构成的多项式环，它的分式域由有理分式$\dfrac{f(x)}{g(x)}$构成($f(x),g(x)\in F[x]$，且 $g(x)\neq 0$)，其加法和乘法按照普通分式运算法则进行.

定理 15.11.8 若 α 是域 F 上的一个代数元素，则

$$F(\alpha)\cong F[x]/(p(x)).$$

这里 $p(x)$是 $F[x]$的一个唯一确定的、首项系数为 1 的不可约多项式而且 $p(\alpha)=0$，因而 $F(\alpha)$的每个元素都可唯一地表成

$\sum_{i=0}^{n-1} a_i\alpha^i$ $(a_i \in F)$ 的形式，其中 n 是 $p(x)$ 的次数. 要把这样的两个多项式 $f(\alpha)$ 和 $g(\alpha)$ 相加，只需把相应的系数相加；$f(\alpha)$ 与 $g(\alpha)$ 的乘积等于 $r(\alpha)$，其中 $r(x)$ 是用 $p(x)$ 除 $f(x)g(x)$ 后所得的余式.

定义 15.11.9 在单代数扩域 $F(\alpha)$ 中，满足条件 $p(\alpha)=0$ 的次数最低的多项式：

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

称为元素 α 的在 F 上的**极小多项式**(minimal polynomial). n 称为 α 在 F 上的**次数**(degree).

以上两个定理回答了单扩域的构造问题. 下面再介绍它们的存在问题和数量问题：对于单超越扩域，由定理 15.10.6 及定理 15.9.1 可知多项式环 $F[x]$及其分式域是存在的且彼此同构.

定理 15.11.10 设 α 是域 F 上的超越元素，将 α 添加到 F 上的单超越扩域是存在的，而且 F 的任何单超越扩域都互相同构.

定理 15.11.11 在同构的意义下，存在且仅存在域 F 的一个单代数扩域 $F(\alpha)$，其中 α 的极小多项式是由 $F[x]$确定的、最高次系数为 1 的不可约多项式(所谓不可约多项式是指不能再分解为次数较低的若干个真正因子的乘积的多项式.)

例 15.11.12 例 15.10.12 的 $\mathbf{Q}[\sqrt{2}]$，实际上是将无理数$\sqrt{2}$添加到有理数域 $\mathbf{Q}$ 的单代数扩域 $\mathbf{Q}(\sqrt{2})$(例 15.11.6)，这时$\sqrt{2}$的极小多项式是 x^2-2，它在 $\mathbf{Q}$ 上的次数是 2；同理复数域 $\mathbf{C}$ 是在实数域 $\mathbf{R}$ 上添加纯虚数 i 所得的单代数扩域 $\mathbf{C}=\mathbf{R}(\mathrm{i})$，其最小多项式是 x^2+1，它在 $\mathbf{R}$ 上的次数也是 2.

15.12 任意域的构造

任何域都可以从素域出发经过有限或无限的单超越扩张或单

代数扩张建立起来，而且有以下事实：设 E 是 F 的一个扩域，并且 E 含有 F 上的超越元素，则总存在 E 的子域 T，使得

$$F \subset T \subset E,$$

且 T 是由 F 添加 F 上的超越元素得到的，而 E 则只包含 T 上的代数元素. 这一事实可从有理数域扩张到复数域时，中间经过某些超越扩域，然后再进行代数扩张而得到认证.

这些事实说明，一个扩域通常可分超越的部分和代数的部分. 我们现仅介绍代数扩域.

定义 15.12.1 若域 F 的扩域 E 的每个元素都是 F 上的代数元素，则 E 叫做 F 的**代数扩域(或代数扩张)**(algebraic extension).

对于代数扩域有以下重要结论.

定理 15.12.2 设 $\alpha_1, \alpha_2, \cdots, \alpha_t$ 是域 F 上的 t 个代数元素，将它们陆续添加到 F 上去所得的扩域 $E = (((F(\alpha_1))\alpha_2)\cdots\alpha_t) = F(\alpha_1, \alpha_2, \cdots, \alpha_t)$ 仍是 F 的代数扩域，因而 E 的每个元素都是 F 上的代数元素.

更为一般的有下面定理.

定理 15.12.3 设集 S 是由域 F 上的代数元素组成的，将 S 添加到域 F 上所得的扩域 $E = F(S)$ 是 F 的代数扩域，因而 E 的每个元素都是 F 上的代数元素.

这两个定理的证明都要用到有限扩域及其有关性质.

定义 15.12.4 设 E 是域 F 的扩域，则对于 E 的加法和 $F \times E$ 到 E 的乘法，E 构成 F 上的一个 n 维向量空间，称 n 为扩域 E 在 F 上的**次数**，记做 $(E:F)$，并称 E 为域 F 的**有限扩域**(finite extension)；否则 E 称为 F 的**无限扩域**(infinite extension).

例 15.12.5 (1) $E = \mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ 是 $\mathbf{Q}$ 的次数为 2 的有限扩域，若将它看成 $\mathbf{Q}$ 上的向量空间时，$\{1, \sqrt{2}\}$ 构成它的一个基，其维数为 2，故 $(E:\mathbf{Q}) = 2$.

（2）实数域 **R** 是有理数域 **Q** 的无限扩域，因为 **R** 是 **Q** 上的无限维向量空间.

有限扩域的次数之间有以下关系.

定理 15.12.6 设 $F, F_1, \cdots, F_t$都是域，其中后一个是前一个的有限扩域，则其次数间有以下关系：

$$(F_t : F) = (F_t : F_{t-1})(F_{t-1} : F_{t-2})\cdots(F_1 : F).$$

在域 F 的代数扩域与有限扩域间有以下结论.

定理 15.12.7 域 F 的单代数扩域 $E = F(\alpha)$必为有限扩域；如果 α 在 F 上的极小多项式的次数为 n，则$(E : F) = n$.

定理 15.12.8 域 F 的有限扩域必为 F 的代数扩域.

利用归纳法及以上三定理即可证明定理 15.12.2 及定理 15.12.3.

注 15.12.9 （1）请注意定理 15.12.2 与定理 15.12.3 的区别，前者添加的代数元素的个数是有限的；后者添加的集 S 可以是有限的，也可以是无限的.

（2）有限扩域必为代数扩域（定理 15.12.8），但 F 上的代数扩域却未必是 F 上的有限扩域，这由于在有理数域 **Q** 上添加全体代数元素所构成的代数扩域并不是 **Q** 的有限扩域.

15.13 代数闭域与多项式的分裂域

初等代数中的代数基本定理说：复数域 **C** 上的一元多项式环 **C**$[x]$中的每一个 n 次多项式在 **C** 里有 n 个根. 换言之，**C**$[x]$中的每一个多项式在 **C**$[x]$里都能分解为一次多项式的乘积.

定义 15.13.1 若域 E 上的多项式环 $E[x]$中的每个多项式都能分解成一次多项式的乘积，则域 E 称为**代数闭域**（algebraically closed field）.

定理 15.13.2 **代数基本定理**（algebraic fundamental theorem）

每个域 F 都有一个代数封闭的代数扩域 E，且在同构的意义下它是唯一确定的（换言之：F 的任意两个代数封闭的代数扩域 E 和 E' 都是同构的）.

本节不证明这个定理，而是通过对多项式的分裂域的讨论看出证明上述定理的途径.

定义 15.13.3 设 E 是域 F 的扩域，$f(x)$ 是 $F[x]$ 的 n 次多项式，若满足以下条件，则称 E 为 $f(x)$ 在 F 上的**分裂域**(splitting field)：

(1) $f(x)$ 在 $E[x]$ 里可以分解为一次多项式的乘积：

$$f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\quad(\alpha_i\in E);$$

(2) 在小于 E 的中间域 $I(F\subset I\subset E)$ 里，$f(x)$ 不能分解为一次多项式的乘积.

由此，E 是一个使得 $f(x)$ 能够分解为一次因子的 F 的最小扩域.

例 15.13.4 (1) x^2+1 作为实数域 $\mathbf{R}$ 上的多项式的分裂域是复数域 $\mathbf{C}$，因为在 $\mathbf{C}$ 内它能分解为一次因子的乘积，且除 $\mathbf{C}$ 外没有包含 $\mathbf{R}(\mathrm{i})$ 的中间域.

x^2+1 作为有理数域 $\mathbf{Q}$ 上的多项式的分裂域是扩域 $\mathbf{Q}(\mathrm{i})$ 而不是 $\mathbf{C}$，因为在 $\mathbf{Q}(\mathrm{i})$ 内 x^2+1 已能分解为 $\mathbf{Q}$ 上的一次因子的乘积.

(2) $x^4-7x^2+10\in\mathbf{Q}[x]$ 分裂域是 $E=\mathbf{Q}(\sqrt{2},\sqrt{5})$，因为在 $E[x]$ 内它能分解为 $(x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{5})(x-\sqrt{5})$，而且在 $\mathbf{Q}$ 与 E 间没有中间域 I 能使它作如上的分解.

定理 15.13.5 若 E 是域 F 上多项式 $f(x)$ 的一个分裂域：

$$f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\ (\alpha_i\in E),$$

则

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n).$$

换言之：$f(x)$ 的分裂域是将它的所有根陆续地添加到 F 上的扩域，因此有些作者亦将 E 称为多项式 $f(x)$ 在 F 上的**根域**(root

field).

定理 15.13.6 设 F 为域，$f(x)\in F[x]$，则存在 $f(x)$ 在 F 上的分裂域.

定理 15.13.6 肯定了 $f(x)$ 在 F 上分裂域的存在性，定理 15.13.7 则保证了分裂域的唯一性.

定理 15.13.7 设 F 与 F' 是两个同构的域，在同构 φ 下：

$$\varphi: a \mapsto a' \quad (\forall a \in F),$$

$$\varphi: f(x)=\sum a_i x^i \mapsto \sum a_i' x^i = f'(x) \quad (\forall f(x)\in F[x]),$$

又设

$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 $f(x)$ 在 F 上的分裂域，

$E'=F'(\beta_1,\beta_2,\cdots,\beta_n)$ 是 $f'(x)$ 在 F' 上的分裂域，

则在 E 与 E' 间存在同构映射 φ_0，将根的次序调整后，有

$$\varphi_0: \alpha_i \mapsto \beta_i.$$

定理 15.13.6 及定理 15.13.7 保证了分裂域的唯一性与存在性. 保证了域 F 上多项式 $f(x)$ 在 F 的某一扩域中一定有 n 个根，而且从构造的观点看它的任何两个分裂域没有本质的区别. 所以分裂域理论在一定意义下体现了代数基本定理的作用.

定理 15.13.8 设 E 是多项式 $f(x)$ 在域 F 上的分裂域，而 β 是 E 的任意元素，则 β 在 F 上的极小多项式 $g(x)$ 在 E 中也可分解为一次因子的乘积.

例 15.13.9 $f(x)=x^2-2\in \mathbf{Q}[x]$，$f(x)$ 在 $\mathbf{Q}$ 上的分裂域是 $E=\mathbf{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in \mathbf{Q}\}$. 从 E 中任取一数 $\beta=a+b\sqrt{2}$，则它在 $\mathbf{Q}$ 上的极小多项式(见定义 15.11.9)是

$$g(x)=x^2-2ax+a^2-2b^2.$$

它能在 E 上作一次因子分解：

$$g(x)=(x-a-b\sqrt{2})(x-a+b\sqrt{2}).$$

15.14 有限域(Galois 域)

有限域又名 Galois 域，是为纪念它的创始人、天才数学家 E. Galois而命名的. 它在方程式论、实验设计和编码理论等方面有广泛的应用.

定义 15.14.1 只含有限个元素的域叫做有限域(finite field)或 **Galois 域**. 若元素个数为 q,常用 $GF(q)$表示.

例 15.14.2 (1) 特征是素数 p 的素域 $\mathbf{Z}_p$(定理 15.11.4)是有限域.

(2) 任一有限域 $GF(q)$的特征必为素数 p,而任一特征为 p 的域必是素域 $\mathbf{Z}_p$的扩域(定理 15.11.4). 由于它是有限域，这个扩域又不能是超越的，因此 $GF(q)$只能是 $\mathbf{Z}_p$的有限扩域. 作为例子，取素域 $\mathbf{Z}_2$及 α 的极小多项式(定义 15.11.9)$p(x)=x^2+x+1$. 根据定理 15.11.8 有：$GF(4)=\mathbf{Z}_2[x]/(x^2+x+1)\cong\mathbf{Z}_2(\alpha)=\left\{\sum_{i=0}^{1}a_i\alpha^i \mid a_i\in\mathbf{Z}_2\right\}=\{0,1,\alpha,\alpha+1\}$,其中 $\alpha^2+\alpha+1=0$(α 满足极小多项式：$x^2+x+1=0$).

$GF(4)$的两种运算表如表 15.3 和表 15.4.

表 15.3

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

表 15.4

·	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

注意：作乘法时要记住 $\alpha^2+\alpha+1=0$ 及在 $\mathbf{Z}_2$ 中 $-\alpha=\alpha$, $-1=1$ 等事实.

定理 15.14.3 设 $GF(q)$的特征为 p,它在素域 Δ 上的次数定义(15.12.4)为 n,则该域的元素个数 $q=p^n$.

例 15.14.2 的 $GF(4)$是本定理的特例.它很容易理解:因为它在 Δ 上的次数为 n 时,则 $GF(q)$作为 Δ 上的向量空间的维数为 n,因而$\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$显然是它的一组基,因此它的每个元都可写成 $a_0+a_1\alpha^1+a_2\alpha^2+\cdots+a_{n-1}\alpha^{n-1}(a_i\in\Delta)$的形式,由于 Δ 只有 p 个元素,每个 a_i只能有 p 种选法,故知 $q=p^n$.

也可根据域的元素决定最小多项式 $p(x)$进而作出所求的有限域.

例 15.14.4 作出域 $GF(125)$.因为 $125=5^3$,所以 $p=5,n=3$,而 $\Delta=\mathbf{Z}_5$.要作出这个域,先找出 α 在 $\mathbf{Z}_5$上的最小多项式 $p(x)=x^3+ax^2+bx+c$.由于三次可约多项式必有一个一次因子,由因子定理可知,$p(x)$是 $\mathbf{Z}_5[x]$上的不可约多项式的充要条件是用 $\mathbf{Z}_5$的元素 $n=0,1,2,3,4$ 代入 $p(x)$时都有 $p(n)\neq 0$.经逐个检验知,$p(x)=x^3+x+1$是一个最小多项式,故 $GF(125)=\mathbf{Z}_5[x]/(x^3+x+1)=\{a_0+a_1\alpha+a_2\alpha^2\mid a_i\in\mathbf{Z}_5\}$.

注:除 x^3+x+1 外还可以有其他最小多项式(如 x^3+x^2+1),但可证明 $\mathbf{Z}_5[x]/(x^3+x+1)$与 $\mathbf{Z}_5[x]/(x^3+x^2+1)$同构.

定理 15.14.5 $GF(p^n)$是多项式 $x^{p^n}-x$ 在其所含素域 Δ 上的分裂域,而且任何两个这样的域(指元素相同的 Galois 域)都同构.

例 15.14.6 可以验证例 15.14.2(2)的 $GF(4)=\{0,1,\alpha,\alpha+1\}$是多项式 x^4-x 在 $\mathbf{Z}_2$上的分裂域,这是因为

$$\begin{aligned}
&(x-0)(x-1)(x-\alpha)(x-\alpha-1)\\
&\quad=(x+0)(x+1)(x+\alpha)(x+\alpha+1)\\
&\quad=(x^2+x)(x^2+x+\alpha^2+\alpha)=(x^2+x)(x^2+x+1)\\
&\quad=x^4+x=x^4-x.
\end{aligned}$$

所以 x^4-x 能分解成 $\mathbf{Z}_2[x]$ 上的一次因子的乘积. 此外, x^4-x 不能在其他中间域里分解. 所以 $GF(4)$ 是 x^4-x 在 $\mathbf{Z}_2$ 上的分裂域.

利用分裂域还可以证明 Galois 域的存在性.

定理 15.14.7 设 Δ 是特征为 p 的素域, 任给整数 $q=p^n(n\geqslant 1)$, 作多项式 x^q-x 在 Δ 上的分裂域 E, 则 E 是有 q 个元素的 Galois 域 $GF(q)$. 因为 x^q-x 的分裂域都是存在的, 所以 $GF(q)$ 总是存在的.

定理 15.14.8 每个 $GF(p^n)$ 都是它的素域 Δ 的单扩域.

定义 15.14.9 循环群 $\langle GF(p^n)^*;\cdot\rangle$ 的生成元称为 $GF(p_n)$ 的**本原元**(primitive element).

设 α 是 $GF(p^n)$ 的一个本原元, 则由定理 15.14.8 可得

$$GF(p^n)^*=\{1,\alpha,\alpha^2,\cdots,\alpha^{p^n-2}\},$$

$$GF(p^n)=\mathbf{Z}_p(\alpha)=\{0,1,\alpha,\alpha^2,\cdots,\alpha^{p^n-2}\}.$$

例 15.14.10 求 $GF(q)=GF(3^2)$ 的所有本原元 α, 这里 $\alpha^2+1=0$. 由于

$$\begin{aligned}GF(9)=\mathbf{Z}_3[x]/(x^2+1)&=\{a+bx\mid a,b\in\mathbf{Z}_3\}\\&=\{0,1,2,\alpha,1+\alpha,2+\alpha,2\alpha,1+2\alpha,2+2\alpha\}.\end{aligned}$$

直接验证得 $1+\alpha,2+\alpha,1+2\alpha$ 及 $2+2\alpha$ 在 $GF(9)^*$ 中的阶是 8, 它们就是 $GF(9)^*$ 的生成元, 因而是 $GF(9)$ 的本原元.

定义 15.14.11 $\mathbf{Z}_p[x]$ 的 m 次不可约多项式 $g(x)$, 若 $g(x)\mid x^{p^m-1}-1$, 而且后者是 $g(x)$ 中的 x^k-1 形的倍式中次数最低的. 则称为**本原多项式**(primitive polynomial)(换言之, $g(x)\nmid x-1$, $g(x)\nmid x^2-1,\cdots,g(x)\nmid x^{p^m-2}-1,g(x)\mid x^{p^m-1}-1$).

例 15.14.12 (1) 例 15.14.2 的 $GF(4)$ 中, $g(x)=x^2+x+1\in\mathbf{Z}_2[x]$ 是一个本原多项式, 因为 $g(x)\mid x^3-1$, 而且 x^3-1 是 $g(x)$ 的 x^k-1 形的倍式中次数最低的.

(2) 例 15.14.10 的 x^2+1 不是 $GF(9)$上的本原多项式,因为虽然有 $x^2+1 \mid x^{9-1}-1$,但后者却不是 x^2+1 中的形如 x^k-1 的倍式中次数最低的(如 x^4-1 就是 x^2+1 的一个倍式).

定理 15.14.13 不可约多项式 $g(x)\in \mathbf{Z}_p[x]$是本原多项式当且仅当它的所有根都是 $\mathbf{Z}_p[x]/(g(x))=GF(p^m)$的本原元.

例 15.14.14 在例 15.14.10 中 x^2+1 不是本原多项式,但 $1+\alpha$,$1+2\alpha(=1-\alpha)$,$2+\alpha$ 及 $2+2\alpha(=2-\alpha)$都是 $GF(9)$的本原元.现求它们的本原多项式:由于

$(x-1-\alpha)(x-1+\alpha)=(x-1)^2-\alpha^2=x^2+x+2\in \mathbf{Z}_3[x]$,

可以验证 x^2+x+2 是所求的本原多项式.

同理可证 x^2+2x+2 是对应于后两个本原元(即 $2+\alpha$,$2+2\alpha$)的本原多项式.

15.15 可分扩域

上节已看到,无论怎样复杂的有限域都可以通过从素域 $\mathbf{Z}_p$ 出发作一个单扩张得到.为了理论的完整性,本节将简约地介绍另一种类型的单扩域,即可分扩域.

定义 15.15.1 设 F 是一个域,E 是 F 的代数扩域,且 $\alpha\in E$,如果 α 在 F 上的极小多项式没有重根,则 α 叫做 F 上的**可分元**(separable element).如果 E 的每一个元素都是 F 上的可分元,则 E 叫做 F 的**可分扩域**(separable extension);否则 E 叫做 F 的**不可分扩域**(non separable extension).

从下述几个定理可知:绝大多数的扩域都是可分扩域,它们的元素都是可分元,仅在极少数的例子中才可看到不可分扩域的存在,例如单超越扩域 $\mathbf{Z}_3(\pi)$就是不可分扩域,但在它里面仍有可能存在可分元.

现将主要结论综述如下.

定理 15.15.2 特征是∞的域的任何代数扩域都是可分扩域.

定理 15.15.3 $GF(p^n)$的任何代数扩域都是可分扩域.

定理 15.15.4 任意域 F 的有限可分扩域 E 必是 F 的单扩域.

15.16 整环中的因子分解

在整数环中,每个整数都能唯一地表成若干个素数的乘积,本节将考虑在一般环中唯一分解定理是否成立.讨论将局限在有单元 1 的交换整环 D 中,并将介绍几种特殊的唯一分解整环,特别是多项式环的因子分解问题.

15.16.1 素元、因子与唯一分解

定义 15.16.1 设 D 是有单元 1 的交换整环,$a,b\in D$,如果$\exists c\in D$使得

$$a=bc,$$

则称 a 被 b **整除**(divisibility),或 b 是 a 的**因子**(divisor/factor),并用符号 $b|a$ 表示.如果 b 不能整除 a 就用符号 $b\nmid a$ 表示.

定义 15.16.2 设 $a,b\in D$,若存在 D 的单位 ϵ 使 $b=a\epsilon$,则称 b 是 a 的**相伴元**(associate)(定理 15.4.6).

例 15.16.3 (1) 在整数环 $\mathbf{Z}$ 里,$3|15$,$3\nmid 16$,又± 1是它仅有的两个单位,因而$\pm 1\cdot a$ 是整数 a 的相伴元.

(2) 在数域 F 上的多项式环 $F[x]$中,$x-1|x^2-1$,但 $x-1\nmid x^2+1$;数域 F 的每个非零的数 a 都是 $F[x]$的单位,因而 $af(x)$是 $f(x)$的相伴元.

定义 15.16.4 单位 ϵ 及元 a 的相伴元 $a\epsilon$ 叫做 a 的**平凡因子**(trivial factor);若 a 还有其他因子,则称为 a 的**真正因子**(proper

factor).

定义 15.16.5 设 $p\in D$，若 p 不是零元，也不是单位，并且只有平凡因子，则称 p 是**素元**(prime element).

例 15.16.6 (1) 在整数环 $\mathbf{Z}$ 中所有素数都是它的素元.

(2) 在数域 F 上的多项式环 $F[x]$ 中，所有不可约多项式 $p(x)$ 都是它的素元.

定理 15.16.7 单位 ε 和素元 p 的乘积 εp 也是 D 的素元.

定义 15.16.8 D 中的元素 a 称作在 D 中有**唯一分解**(unique factorization)，若满足以下两个条件：

(1) 它能分解成有限多个素元的乘积：

$$a = p_1 p_2 \cdots p_r \quad (p_i \text{ 是 } D \text{ 的素元});$$

(2) 若还有另一个有限素元分解：

$$a = q_1 q_2 \cdots q_s \quad (q_i \text{ 是 } D \text{ 的素元}),$$

则必有 $r=s$，而且将 q_i 经过次序调整后就可使 $q_i=\varepsilon_i p_i$.

由定义可见，整环 D 里的零元素和单位都不能作唯一分解(否则其分解中含有零元素或单位，而零元素和单位都不是素元，因而其分解不是有限素元分解)，因而在讨论因子分解时要把它们排除出去.

例 15.16.9 (1) 整数环 $\mathbf{Z}$ 中每个不等于 0 和 1 的整数都能作唯一分解.

(2) 数域 F 上的一元多项式环 $F[x]$ 的每个非零次的非零多项式都能分解成若干个不可约多项式的乘积，经调整次序后，这些不可约多项式最多只能差一个常数因子($F[x]$ 的单元).

(3) 在某些含单元 1 的交换整环 D 中确有元素不能作唯一分解. 例如 Gauss 整数环 $D=\{a+b\sqrt{-3}\,|\,a,b\in\mathbf{Z}\}$ 中的数 4 可有两种分解：

$$4 = 2\cdot 2 = (1+\sqrt{-3})\cdot(1-\sqrt{-3}),$$

而 2 及 $1\pm\sqrt{-3}$都是 D 的素元.

15.16.2 唯一分解整环

定义 15.16.10 若一个有单元 1 的交换整环 D 的每个不等于零和单位的元素都有唯一分解，则 D 称作**唯一分解整环**(unique factorization domain)或 Gauss **整环**(Gauss domain).

例 15.16.11 整数环 $\mathbf{Z}$ 及数域 F 上的多项式环 $F[x]$都是唯一分解整环.

唯一分解整环有以下重要性质.

定理 15.16.12 (1) 设 D 是唯一分解整环，且 $p,a,b\in D$，而 p 是素元，则由 $p|a\cdot b$，可得 $p|a$ 或 $p|b$.

(2) 设 D 是有单元 1 的交换整环，对 D 中任意元素 a,b，任意素元 p，若由 $p|a\cdot b$ 就可推得 $p|a$ 或 $p|b$，则 D 的每个不是零和单元的元素必有唯一分解，因而 D 是一个唯一分解整环.

定义 15.16.13 设 $a_1,a_2,\cdots,a_n,c\in D$，若 $c|a_1,a_2,\cdots,a_n$，则称 c 是 $a_1,a_2,\cdots,a_n$的**公因子**(common factor).

在 $a_1,a_2,\cdots,a_n$的公因子中，如果公因子 d 能被它们的每个公因子 c 整除，则称 d 为 $a_1,a_2,\cdots,a_n$ 的**最大公因子**(greatest common factor)，用 $d=(a_1,a_2,\cdots,a_n)$表示.

定理 15.16.14 设 $a_1,a_2,\cdots,a_n$是唯一分解整环 D 的 n 个元素，则在 D 中必定有它们的最大公因子 d，而且它们的任何两个最大公因子 d 与 d'最多只能差一个单位因子，即 $d=\varepsilon d'$(ε 是单位).

要求两个整数或两个多项式的最大公因子通常使用**欧几里得算法**(Euclid algorithm)又称**辗转相除算法**，但在一般环中，特别是求多个元素的最大公因子时，则常利用各 a_i的标准分解式 $a_i=\varepsilon_i p_1^{h_1}p_2^{h_2}\cdots p_n^{h_n}$ (ε_i是单位，$h_j\geqslant 0$)，令 l_j是同一个 p_j 的上方指数的最小的一个，则 $d=p_1^{l_1}p_2^{l_2}\cdots p_n^{l_n}$ 即为所求的最大公因子.

利用最大公因子可以定义互素的概念.

定义 15.16.15 设 $a_1,a_2,\cdots,a_n$ 是唯一分解整环 D 的 n 个元素，如果它们的最大公因子是单位，则称这 n 个**元素互素**(prime to each other).

特别地，若它们中每两个元素的最大公因子都是单位 1，即

$$(a_i,a_j)=1 \quad (i \neq j, i,j=1,2,\cdots,n),$$

则称这 n 个元素**两两互素**.

要判断一个整环是否是唯一分解整环是相当困难的，作为例子，下面介绍两种类型的唯一分解整环，它们是主理想整环和欧氏整环.

定义 15.16.16 设 D 是有单元 1 的交换整环，如果它的每个理想都是主理想，则称 D 为**主理想整环**(principal ideal domain).

定义 15.16.17 设 D 是有单元 1 的交换整环，如果它能满足以下两个条件，则称 D 为**欧氏整环**(Euclid domain).

(1) 有一个从 D 的非零元素集 D' 到非负整数集 $\mathbf{N}$ 的映射 $\varphi: D' \to \mathbf{N}$；

(2) 给定 D 的一个非零元素 a，D 的任何元素 b 都可以写成

$$b = qa + r \qquad (q,r \in D)$$

的形式，其中或者 $r=0$ 或者 $r<a$.

定理 15.16.18 主理想整环、欧氏整环都是唯一分解整环.

15.16.3 多项式环的因子分解

在例 15.16.11 中已知数域 F 上的多项式环 $F[x]$ 是唯一分解整环，而且，F 上的多元多项式环、甚至一般域上的一元和多元多项式环都是唯一分解整环；不仅如此，还可以把它推广到有单元 1 的交换整环上去，可以证明以下定理.

定理 15.16.19 设 D 是有单元 1 的交换整环，$x_1,x_2,\cdots,x_n$ 是 D 上的独立超越元素，则 $D[x_1]$，$D[x_1,x_2]$，$\cdots$，$D[x_1,x_2,\cdots,x_n]$ 都是唯一分解整环.

15.17 环论在编码理论中的应用

本节是 14.12 节编码理论的继续，利用多项式环及有限域理论作为研究工具，得到两种重要而有效的码——多项式码和 BCH 码.

15.17.1 多项式码

定义 15.17.1 设 $\boldsymbol{a}=a_0a_1\cdots a_{n-1}\in B_2^n$ 是一个码字，则以它的码元为系数的多项式.

$\boldsymbol{a}(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}\in \mathbf{Z}_2[x]$，叫做码字 $\boldsymbol{a}$ 的**多项式表示法**(polynomial representation)（注意多项式是按升幂排列的，且下标从 0 开始!）.

定义 15.17.2 设 $g(x)=g_0+g_1x+\cdots+g_kx^k\in \mathbf{Z}_2[x]$ $(g_0,g_k\neq 0)$ 是一个给定的 k 次多项式，$\boldsymbol{a}=a_0a_1\cdots a_{m-1}\in B_2^m$ 是一个长为 m 的信息字，而且 $m+k=n$. 将 $\boldsymbol{a}(x)$ 与 $g(x)$ 相乘，设其积为

$$\begin{aligned}\boldsymbol{b}(x)&=\boldsymbol{a}(x)\cdot g(x)\\&=b_0+b_1x+b_2x^2+\cdots+b_{n-1}x^{n-1}\in \mathbf{Z}_2[x],\end{aligned}$$

根据这个乘积及相应系数作编码函数

$$E:\boldsymbol{a}=a_0a_1\cdots a_{m-1}\mapsto \boldsymbol{b}=b_0b_1\cdots b_{n-1},$$

则此 (n,m) 码叫做由 $g(x)$ 生成的**多项式码**(polynomial code).

注意：(1) 这里规定 $g(x)$ 的系数 g_0 及 g_k 均不为零，否则将有 $b_0=0$ 或 $b_{n-1}=0$，这就浪费了码字的位数.

(2) 这个定义完全可以推广到任意有限域 $GF(q)$ 上去，比如 $\mathbf{Z}_3$ 或 $\mathbf{Z}_5$；但因实际上的计算设备是双稳态的，因此仅用到 $\mathbf{Z}_2$.

例 15.17.3 设 $g(x)=1+x^2+x^3$，可作 $(8,5)$ 码如下：任取信息字 $\boldsymbol{a}=a_0a_1\cdots a_4\in B_2^5$，作多项式乘积：

$\boldsymbol{b}(x)=\boldsymbol{a}(x)\cdot g(x)$

$$=(a_0+a_1x+\cdots+a_4x^4)(1+0\cdot x+x^2+x^3)$$
$$=b_0+b_1x+\cdots+b_7x^7,$$

则编码函数是

$$E:\boldsymbol{a}=a_0a_1\cdots a_4\mapsto\boldsymbol{b}=b_0b_1\cdots b_7.$$

现作一具体的例:取 $\boldsymbol{a}=01011$,则 $\boldsymbol{a}(x)=x+x^3+x^4$,而 $\boldsymbol{b}(x)=\boldsymbol{a}(x)\cdot g(x)=x+x^5+x^7$,因而 $\boldsymbol{b}=01000101$ 是与 $\boldsymbol{a}$ 相应的码字.

由多项式的乘法可见:

定理 15.17.4 一个由编码多项式

$$g(x)=g_0+g_1x+g_2x^2+\cdots+g_kx^k$$

生成的多项式码是一个 $m\times(m+k)$ 矩阵

$$\boldsymbol{G}=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{k-1} & g_k & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & g_0 & g_1 & \cdots & g_{k-1} & g_k \end{bmatrix}$$

为编码矩阵的矩阵码,$g_0,g_1\cdots,g_k$依次在矩阵的每一行上出现,它们从第 j 行上的第 j 位开始一直延伸到第 $j+k$ 位上.换言之,每行上的 $g_0,g_1,\cdots,g_k$实际上是将上一行的每个元向右下角移一位的结果.

例 15.17.5 由码多项式 $1+x+x^3$ 及三位信息字作成的(6,3)多项式码的编码矩阵是

$$\boldsymbol{G}=\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

对应于每个信息字 $\boldsymbol{a}$ 其相应的码字可列表如下:

$\boldsymbol{a}\mapsto\boldsymbol{b}=\boldsymbol{aG}$[①]

---

① $\boldsymbol{aG}$ 的运算是将 $\boldsymbol{a}=a_1a_2a_3=(a_1,a_2,a_3)$ 视 a 为行向量与矩阵 $\boldsymbol{G}$ 进行乘法运算的结果.

000 ↦ 000000	100 ↦ 110100
001 ↦ 001101	101 ↦ 111001
010 ↦ 011010	110 ↦ 101110
011 ↦ 010111	111 ↦ 100011

定理 15.17.6 多项式码都是群码(定义 14.12.33)，以 $g(x)$ 为编码函数的多项式码的最小距离(定义 14.12.13)等于它的某个非零码字的重，这个重是所有非零码字的重中的最小的(定理 14.12.35).

例 15.17.5 的以 $1+x+x^3$ 为编码函数的(6,3)码的最小距离是 3，恰是它的非零码字 001101 的重.

定理 15.17.7 在 $\mathbf{Z}_2[x]$中，$1+x$ 的每个倍式必定包含偶数个非零项，因此任一以 $1+x$ 的倍式 $g(x)=(1+x)h(x)$ 为编码函数的多项式码必包含偶数个 1，从而构成一个奇偶校验码(例 14.12.10)，它能检出奇数个传输错误.

例 15.17.8 利用编码多项式 $g(x)=1+x$ 可生成一个 $(n,n-1)$ 奇偶校验码. 以 $n-1=3$ 为例说明之. 此时信息字 $\boldsymbol{a}=a_0a_1a_2$，编码矩阵为

$$\boldsymbol{G}=\begin{bmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\end{bmatrix},$$

编码表如下：

$\boldsymbol{a}\mapsto\boldsymbol{b}=\boldsymbol{aG}$

000 ↦ 0000	100 ↦ 1100
001 ↦ 0011	101 ↦ 1111
010 ↦ 0110	110 ↦ 1010
011 ↦ 0101	111 ↦ 1001

这确是一个(4,3)奇偶校验码，它的每个码字都含有偶数个 1，因此能检验传输中出现的任何奇数个错误.

下面介绍利用本原多项式(定义 15.14.11)生成多项式码的方法,使得这种码能检出单错、双错或三重错. 为了使校验位减至最少,此生成多项式的次数应该尽可能地小.

定理 15.17.9 (1) 如果 $p(x)$是一个 k 次本原多项式,则由 $p(x)$生成的$(n,n-k)$码能检出所有的单错和双错,其中 $n\leqslant 2^k-1$.

(2) 设 $p_1(x)$ 是一个 k 次本原多项式,则由 $p(x)=(1+x)p_1(x)$生成的$(n,n-k-1)$码能检出所有的双错及任何奇数个错误,其中 $n\leqslant 2^k-1$.

例 15.17.10 (1) 多项式 $1+x^2+x^3\in \mathbf{Z}_2[x]$是 3 次本原多项式,因为它不可约(否则能分解出一个一次因子,由因子定理知它必有一根,但用 $\mathbf{Z}_2$的元 0,1 代入时它都不为 0),而且它能整除 $x^{2^3-1}-1(=x^7-1)$但却不能整除 $x-1,x^2-1,x^3-1,x^4-1,x^5-1$ 及 x^6-1.

利用 $1+x^2+x^3$作(7,4)码如下:

$0000\mapsto 0000000$ $\qquad$ $1000\mapsto 1011000$

$0001\mapsto 0001011$ $\qquad$ $1001\mapsto 1010011$

$0010\mapsto 0010110$ $\qquad$ $1010\mapsto 1001110$

$0011\mapsto 0011101$ $\qquad$ $1011\mapsto 1000101$

$0100\mapsto 0101100$ $\qquad$ $1100\mapsto 1110100$

$0101\mapsto 0100111$ $\qquad$ $1101\mapsto 1111111$

$0110\mapsto 0111010$ $\qquad$ $1110\mapsto 1100010$

$0111\mapsto 0110001$ $\qquad$ $1111\mapsto 1101001$

相应的编码矩阵为

$$\boldsymbol{G}=\begin{bmatrix}1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}.$$

由上可见此码的最小距离为3，据定理14.12.16知此码能检出所有的单错和双错.

(2) $1+x^3+x^{10}\in \mathbf{Z}_2[x]$是10次本原多项式，取$n=2^{10}-1=1023$并以$p(x)=(1+x)(1+x^3+x^{10})$为编码多项式的(1023，1012)多项式码有11个校验位，长为1012的不同的信息字共有2^{1012}个(这是一个"天文数字"，用十进制数表示时有305位!)，它能检出单错、双错、三重错以及任何奇数个错.

(3) 为便于使用，现列出$\mathbf{Z}_2[x]$上的10次以内的本原多项式，如表15.5.

表 15.5

次数 k	2^k-1	本原多项式
1	1	$1+x$
2	3	$1+x+x^2$
3	7	$1+x+x^3$
4	15	$1+x+x^4$
5	31	$1+x^2+x^5$
6	63	$1+x+x^6$
7	127	$1+x^3+x^7$
8	255	$1+x^2+x^3+x^4+x^8$
9	511	$1+x^4+x^9$
10	1023	$1+x^3+x^{10}$

15.17.2 BCH码

这是目前威力较大的一种纠错码，它是1960年左右由Bose、Chaudhuri及Hocquenghem三人独立发现的一种多项式码，简称

BCH 码. 它断言,对于任何正整数 k 及 t,只要 $t<2^{k-1}$,则必然存在一个长为 $n=2^k-1$ 的 BCH 码,它能纠正 t 个或较 t 少的错误. 它是多项式码,其生成多项式 $p(x)$ 的次数 $\leqslant kt$,其信息字长至少为 $n-kt$.

定义 15.17.11 长为 $n=2^k-1$ 的**纠 t-错 BCH 码**(t-error-correcting BCH code)是一个由生成多项式 $p(x)$ 生成的多项式码,这个 $p(x)$ 构成如下:任取 $GF(2^m)$ 的一个本原元(定义 15.14.9)α,设 $p_i(x)\in \mathbf{Z}_2[x]$ 是以 α^i 为根的不可约多项式,则

$$p(x)=\mathrm{LCM}(p_1(x),p_2(x),\cdots,p_{2t}(x)),$$

其中 LCM 表示各多项式的最小公倍式.

注意:(1) 显然 $\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{2t}$ 都是 $p(x)$ 的根,因为 $GF(2^m)$ 的特征是 2,由定理 15.6.5(2) 知 $[p_i(x)]^2=p_i(x^2)$,从而 α^{2i} 是 $p_i(x)$ 的一个根,因此定义中的 $p(x)$ 可简化为

$$p(x)=\mathrm{LCM}(p_1(x),p_3(x),\cdots,p_{2t-1}(x)),$$

这时 $p_2(x),p_4(x),\cdots,p_{2t-2}(x),p_{2t}(x)$ 都可省掉.

(2) 注意纠 t-错码仅算到 $p_{2t}(x)$ 为止.

(3) $p(x)$ 的次数 $\leqslant kt$.

例 15.17.12 找出长为 $n=15$,$t<8$ 的各个纠 t-错 BCH 码.

解 先求出 $GF(16)$ 的 15 个非零元素用本原元 α 方幂表出的式子:由例 15.17.10(3) 知,$1+x+x^4$ 是 $GF(16)$ 的一个本原多项式. 将 α 代入后得 $\alpha^4=1+\alpha$,现陆续求 α 的方幂得 $\alpha,\alpha^2,\alpha^3,\alpha^4=1+\alpha$,$\alpha^5=\alpha\cdot\alpha^4=\alpha(1+\alpha)=\alpha+\alpha^2$,$\alpha^6=\alpha\cdot\alpha^5=\alpha(\alpha+\alpha^2)=\alpha^2+\alpha^3$,$\alpha^7=\alpha^3+\alpha^4=\alpha^3+(1+\alpha)=1+\alpha+\alpha^3$. 类似地计算得

$\alpha^8=1+\alpha^2$,$\alpha^9=\alpha+\alpha^3$,$\alpha^{10}=1+\alpha+\alpha^2$,$\alpha^{11}=\alpha+\alpha^2+\alpha^3$,$\alpha^{12}=1+\alpha+\alpha^2+\alpha^3$,$\alpha^{13}=1+\alpha^2+\alpha^3$,$\alpha^{14}=1+\alpha^3$,$\alpha^{15}=1$.

进一步求以 α^i 为根的 $p_i(x)$,由上面的说明知只须求 i 为奇数的 $p_i(x)$ 即可.

$p_1(x)$显然是 x^4+x+1.

若 $p_3(x)$以 α^3 为根,则它也以 α^6,α^{12},$\alpha^{24}=\alpha^9$ 及$(\alpha^9)^2=\alpha^{18}=\alpha^3$ 为根,因而

$$p_3(x)=(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$$
$$=x^4+x^3+x^2+x+1,$$

$p_5(x)$有根 α^5,α^{10}及 $\alpha^{20}=\alpha^5$,因此

$$p_5(x)=(x-\alpha^5)(x-\alpha^{10})=x^2+x+1,$$

$p_7(x)$有根 α^7,α^{14},$\alpha^{28}=\alpha^{13}$,$\alpha^{26}=\alpha^{11}$及 $\alpha^{22}=\alpha^7$,因此

$$p_7(x)=(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})$$
$$=x^4+x^3+1.$$

至此已穷尽了所有的本原多项式,因为 $p_9(x)=p_3(x)$,$p_{11}(x)=p_{13}(x)=p_7(x)$.

现在就可按照纠正错误的个数写出所用的生成多项式:

(1) 纠 1-错 BCH 码可由 $p(x)=p_1(x)=x^4+x+1$ 生成;

(2) 纠 2-错 BCH 码可由 $p(x)=\mathrm{LCM}(p_1(x),p_3(x))=(x^4+x+1)(x^4+x^3+x^2+x+1)=x^8+x^7+x^6+x^4+1$ 生成;

(3) 纠 3-错 BCH 码可由 $p(x)=\mathrm{LCM}(p_1(x),p_3(x),p_5(x))=(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)=x^{10}+x^8+x^5+x^4+x^2+x+1$ 生成;

(4) 纠 4-错 BCH 码可由 $p(x)=\mathrm{LCM}(p_1(x),p_3(x),p_5(x),p_7(x))=p_1(x)\cdot p_3(x)\cdot p_5(x)\cdot p_7(x)=\frac{x^{15}+1}{x+1}=\sum_{i=0}^{14}x^i$ 生成,注意这个多项式以 $GF(16)$中的 0 和 1 以外的元素为根.

(5) 由于 $p_9(x)=p_3(x)$,纠 5-错 BCH 码可由 $p(x)=\mathrm{LCM}(p_1(x),p_3(x),p_5(x),p_7(x),p_9(x))=\frac{x^{15}+1}{x+1}=\sum_{i=0}^{14}x^i$ 生成,该多项式同时也是纠 6-错、纠 7-错 BCH 码、现将上述结果列于表 15.6.

表 15.6

纠错数 t	$p_{2t-1}(x)$的根	$p_{2t-1}(x)$次数	$p(x)$	$p(x)$次数 $=15-m$	信息字长 m
1	$\alpha,\alpha^2,\alpha^4,\alpha^8$	4	$p_1(x)$	4	11
2	$\alpha^3,\alpha^6,\alpha^{12},\alpha^9$	4	$p_1(x)p_3(x)$	8	7
3	α^5,α^{10}	2	$p_1(x)p_3(x)p_5(x)$	10	5
4	$\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}$	4	$\dfrac{x^{15}+1}{x+1}$	14	1
5	$\alpha^9,\alpha^3,\alpha^6,\alpha^{12}$	4		14	1
6	$\alpha^{11},\alpha^7,\alpha^{14},\alpha^{13}$	4		14	1
7	$\alpha^{13},\alpha^{11},\alpha^7,\alpha^{14}$	4		14	1

说明:纠 2-错 BCH 码是一个(15,7)码,它由 $x^8+x^7+x^6+x^4+1$ 生成,共有 7 个信息位和 8 个校验位;又由$\dfrac{x^{15}+1}{x+1}$生成的纠 7-错 BCH 码是一个(15,1)码,其信息位长为 1,该码共有两个码字:一个由 15 个 0 组成,另一个则由 15 个 1 组成.译码时运用"多者优先"原则进行,即当 1 的个数多于 0 的个数时信息取为 1;反之,当 0 的个数多于 1 的个数时信息取为 0,显然此种码能纠正 7 个错误.

定理 15.17.13 设 t 是小于 2^{k-1} 的正整数,则 BCH 码的任意两个码字间的最小距离为 $2t+1$,因而该码能纠正 t 个以内的所有错误.

例 15.17.14 BCH(127,92)码能纠正 1 至 5 个错误;这种码包含 92 个信息位和 35 个校验位从而包含 2^{35} 个校验子(定义 14.12.26).这是一个庞大的数字,不可能将这些校验子及它们的陪集头全部储存到计算机中去,因而译码问题必须另找其他办法(前段的多项式码也存在同样问题).其实 BCH 码的错误是可以利用代数工具而不必列出校验子和陪集头表就可以发现,因此需

要掌握一套简易代数译码算法，详细论述可参考有关文献.

15.18 拉丁方与有限几何学

拉丁方是一种特殊的幻方，最先把拉丁方应用于农业实验方面的是英国数学家 R. A. Fisher，随后在试验设计中获得大量的应用. 近年来，无论是在对原子的探索，核反应堆中物质的摆放，以及市场经济与社会学等领域中，拉丁方都有有价值的应用!

此外拉丁方与有限几何学以及有限域的理论都有密切的联系.

定义 15.18.1 设 S 是含有 n 个元素的集，这些元素构成一个 $n\times n$ 矩阵 $\boldsymbol{L}=(l_{ij})$，如果 S 的每个元素，在每行中和在每列中恰好出现一次，则该矩阵就叫做 S 上的 n 阶**拉丁方**(Latin square).

例 15.18.2 表 15.7 是集合$\{a,b,c\}$上的 3 阶拉丁方:

表 15.7

a	b	c
c	a	b
b	c	a

定理 15.18.3 任何 n 阶有限群$\langle G;+\rangle$的运算表必是基集 G 上的 n 阶拉丁方. 但其逆未必真.

例 15.18.4 由定理 14.10.11 可知，5 阶群的构造是唯一的，它是一个循环群，因此与模 5 同余类加群$\langle \mathbf{Z}_5;+\rangle$同构，其运算如表 15.8. 从表中可看出，群的每个元在每行(列)上恰好出现一次，所以这个表是一个拉丁方.

表 15.8

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

对于一般的有限群运算表也有类似的情况，因为如果在它的第 i 行上有二个元素 l_{ij} 与 l_{ik} 相同，即 $x_i+x_j=x_i+x_k$. 由于加群中负元素的存在故有 $x_j=x_k$，这就是说每个元素恰好在同一行上出现一次；同理可证每个元素恰好在同一列上出现一次.

该命题元逆不成立，可由下例看到：仍取 $S=\{0,1,2,3,4\}$，则表 15.9 是 S 上的一个 5 阶拉丁方，但却不是一个群. 因为 5 阶群只能有表 15.8 的运算表或把运算表经过行列互换所得的表，但表 15.9 是无论如何也不能由表 15.8 经过行列互换而成.

表 15.9

0	1	2	3	4
1	0	4	2	3
2	3	0	4	1
3	4	1	0	2
4	2	3	1	0

定义 15.18.5 设 L_1 与 L_2 是集 S 上的两个 n 阶拉丁方，如果将它们迭合时，L_1 的每个元仅与 L_2 的每个元接触一次，则称 L_1 与 L_2 是**正交的拉丁方**(orthogonal Latin square).

例 15.18.6 (1) 设有 3 种标号是 a,b,c 的稻种及 3 种不同的土壤 A,B,C. 为了考察土壤肥力对于稻种的影响，划出 9 块土地使这 3 种土壤各种上这 3 种稻种中的某一种，则可用拉丁方表

示其实验方案如表 15.10.

表 15.10

a	b	c	A	B	C
c	a	b	B	C	A
b	c	a	C	A	B

表 15.11

aA	bB	cC
cB	aC	bA
bC	cA	aB

易见表 15.10 中的两个拉丁方是正交的，因为它们的迭合(表 15.11)使第一个表的每个元仅与第二个表的每个元接触一次.

(2) 如果在上面的试验中尚须检验 3 种杀虫剂的效应，是否能找出另一拉丁方使与上面的两个拉丁方相互正交. 回答是否定的. 可以证明：**最多只能有 $n-1$ 个相互正交的 n 阶拉丁方**(见定理 15.18.8). 因此若将上述问题改变成为有 4 种不同的稻种，4 种不同的土壤及 4 种不同的杀虫剂，则作 3 个相互正交的拉丁方是可能的.

定义 15.18.7 若 $L_1,\cdots,L_r$ 都是 n 阶拉丁方而且对于所有 $i\neq j$ 都有 L_i 与 L_j 正交，则称集 $\{L_1,\cdots,L_r\}$ 为 r 个**相互正交的 n 阶拉丁方集**(mutually orthogonal Latin square).

下面介绍从有 n 个元素的有限域 $GF(n)$ 出发作出 $n-1$ 个相互正交的 n 阶拉丁方的方法. 由定理 15.14.3 知，任一有限域有 p^m 个元，即其元数仅是某一素数 p 的方幂. 因此只能构造 $n=2,3,4,5,7,8,9,11,13,16,17,\cdots$ 的拉丁方.

定理 15.18.8 Bose 定理 设 $GF(n)=\{x_0,x_1,\cdots,x_n\}$ 是 n 阶($n=p^m$)有限域，其中 $x_0=0,x_1=1$，则有：

(1) 加法表 $L_1=(a_{ij}^1)$ 是 n 阶拉丁方，其中 $a_{ij}^1=x_i+x_j\quad(0\leqslant i,j\leqslant n-1)$.

(2) 对于 $1<k\leqslant n-1$，作 $L_k=(a_{ij}^k)$ 如下：

$$a_{ij}^k = x_k\cdot x_i + x_j \quad (0\leqslant i\cdot j\leqslant n-1),$$

则每个这样作出的 L_k 是 $GF(n)$ 上的一个 n 阶拉丁方.

(3) $\{L_1, L_2, \cdots, L_{n-1}\}$ 是一个相互正交的 $n(=p^m)$ 阶拉丁方集.

例 15.18.9 (1) 从 $\mathbf{Z}_3$ 出发运用上述定理. 可作出相互正交的两个 3 阶拉丁方如表 15.12.

表 15.12

L_1

0	1	2
1	2	0
2	0	1

L_2

0	1	2
2	0	1
1	2	0

(2) 从 $GF(4)=\mathbf{Z}_2(\alpha)=\{0,1,\alpha,\alpha^2\}$(其中 $\alpha^2=\alpha+1$)出发可作 3 个相互正交的 4 阶拉丁方 L_1, L_2, L_3: L_1 就是 $GF(4)$ 的加法表;仿定理 15.18.8(2)可作出 L_2,其实它也可由用 α 乘 L_1 的第 1 列、然后将 L_1 的行按第 1 列指出的顺序进行置换得到;至于 L_3 也可用 α^2 乘 L_1 的第 1 列后将 L_1 的行按第 1 列指示的顺序进行置换得到. 表 15.13 所示是 3 个相互正交的 4 阶拉丁方:

表 15.13

L_1

0	1	α	α^2
1	0	α^2	α
α	α^2	0	1
α^2	α	1	0

L_2

0	1	α	α^2
α	α^2	0	1
α^2	α	1	0
1	0	α^2	α

L_3

0	1	α	α^2
α^2	α	1	0
1	0	α^2	α
α	α^2	0	1

如果将 a 代替 0, b 代替 1, c 代替 α 及 d 代替 α^2 并将它们迭合即得表 15.14 所示.

表 15.14

aaa	*bbb*	*ccc*	*ddd*
bcd	*adc*	*dab*	*cba*
cdb	*dca*	*abd*	*bac*
dbc	*cad*	*bda*	*acb*

下面介绍有限几何学与拉丁方的关系. 前者是 R. C. Bose 在发表构造 $n-1$ 个相互正交的 n 阶拉丁方的方法时提出的,我们所考虑的有限几何学也仅限于仿射平面.

定义 15.18.10 由点集 P 与线集 L 组成的系统 $\langle P,L\rangle$,若能满足下列三个**关联公理**(incidence axiom),则称为**仿射平面**(affine plane):

(1) 任意两个不同点恰在一条线上;

(2) 对于每一直线 l 及不在 l 上的点 x,存在唯一的一条包含 x 而不与 l 相交的线 m;

(3) 存在着不在一条线上的三点.

定义 15.18.11 设 l, m 是两条线,规定**平行关系**(parallelism)为:直线 l,m 平行的充要条件是 $l=m$ 或 l 与 m 无公共点,记作 $l/\!/m$.

显然平行关系"//"是线集 L 上的等价关系. 而公理(2)断言:过线外一点只能作一条线与另一条线平行.

例 15.18.12 (1) 欧氏平面 $\mathbf{R}^2$ 中的点与直线构成一个有无限多个点的仿射平面.

(2) 图 15.1 是仅有 4 个点的仿射平面,其点集 $P=\{a,b,c,d\}$,而线集 $L=\{\{a,b\},\{c,d\},\{a,c\},\{b,c\},\{b,d\},\{a,d\}\}$.

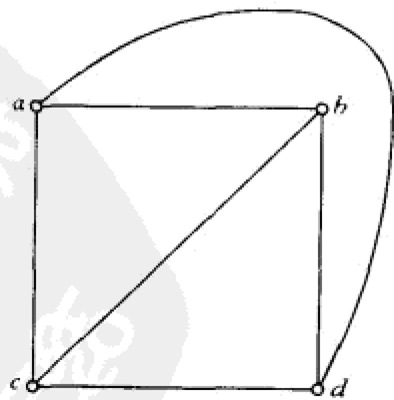


图 15.1

定理 15.18.13 若一个几何系统仅包含有限多个点,则必存在一整数 n 使得该几何系统包含 n^2 个点及 n^2+n 条线,而且每条线都包含 n 个点且每个点都在 $n+1$ 条线上.

定义 15.18.14 定理 15.18.13 的有限几何称为 ***n* 阶仿射平面**

(affine plane of order n).

(图 15.1 的有 4 个点的几何是一个 2 阶仿射平面，它有 6 条线，每条线都包含 2 个点，而每个点都在 3 条线上.)

定理 15.18.15 平行关系是一个等价关系，由该等价关系所确定的划分称为**平行类**(parallelism class). 在一个 n 阶仿射平面内共有 $n+1$ 个平行类.(在图 15.1 中，$\{a,b\}/\!/\{c,d\}$，$\{a,c\}/\!/\{b,d\}$，$\{b,c\}/\!/\{a,d\}$，所以这个 2 阶仿射平面共有 3 个平行类.)

至此可以考虑 n 阶仿射平面与相互正交的 n 阶拉丁方之间的关系.

定理 15.18.16 存在 n 阶仿射平面的充要条件是存在 $n-1$ 个相互正交的 n 阶拉丁方.

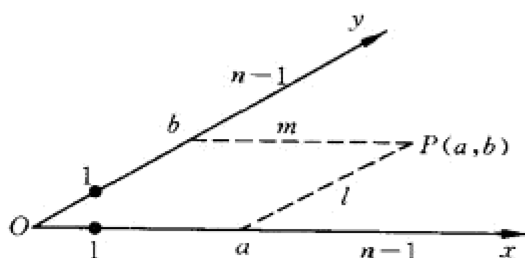


图 15.2

该定理的证明大致如下：设存在一个 n 阶仿射平面，可以仿照通常的坐标法建立“仿射坐标系”，如图 15.2. 过 x 轴上的点 a 作平行于 y 轴的线 l，过 y 轴上的点 b 作平行于 x 轴的线 m. 设 l 与 m 相交于点 P，则 P 的坐标定义为 (a,b). 这时整个坐标平面共有 n^2 个点，它们对应着 n^2 个有序对 (a,b). 这 n^2 个点也对应着 $n\times n$ 正方形的 n^2 个孔，其中 (a,b) 对应于第 a 行的第 b 个孔. 利用定理 15.18.8 的方法即可作出 $n-1$ 个相互正交的 n 阶拉丁方. 这就证明了相互正交的 n 阶拉丁方的存在性.

反之，若存在一个含 $n-1$ 个相互正交的 n 阶拉丁方集时，则

可以将其元素进行编号，因而使这些拉丁方成为 $S=\{0,1,2,\cdots,n-1\}$ 上的拉丁方，然后将 S^2 作为点集并规定 n 个点的集在一条线上的意义，即可证明它是一个 n 阶仿射平面.

例 15.18.17 当 $n=p^m$ 时，可构造有限域 $GF(n)$ 上的 n 阶仿射平面如下：

点集 $P=GF(n)^2=\{(x\cdot y)\mid x,y\in GF(n)\}$；

直线 l 由满足系数在 $GF(n)$ 上的含 x,y 的一个线性方程的一切点组成；

一条线的斜率按通常的定义，它是 $GF(n)$ 的一个元素或无限大；

二线平行当且仅当它们有相同的斜率.

现举特例如下：设 $GF(4)=\mathbf{Z}_2(\alpha)=\{0,1,\alpha,\alpha^2\}$，则 4 阶仿射平面的 16 个点可用图 15.3 表出. 它的水平线可表成

$y=$ 常元，

它们的斜率为 0；至于各垂直线则可表成：

$x=$ 常元，

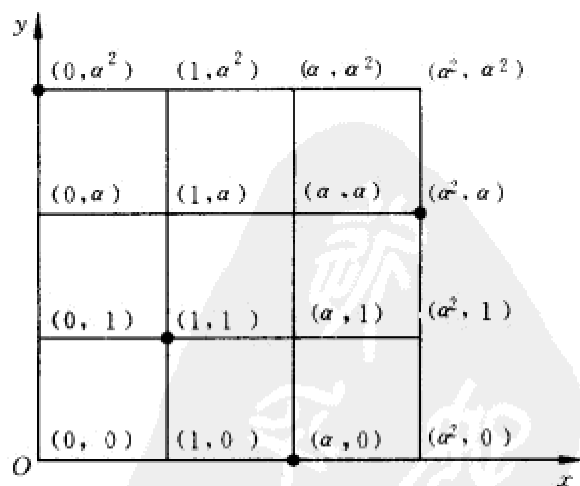


图 15.3

它们的斜率为∞. 特别地，线

$$y = \alpha x + \alpha^2$$

有斜率 α 且包含$(0,\alpha^2)$，$(1,1)$，$(\alpha,0)$及(α^2,α)等 4 个点，它与线 $y=\alpha x$，$y=\alpha x+1$ 及 $y=\alpha x+\alpha$ 平行.

采用例 15.18.9 的方法即可得到与这个 n 阶仿射平面相应的 3 个相互正交的 4 阶拉丁方(表 15.13).

16 模

前两章讨论的代数结构都是由一个集和它上面的一个或两个代数运算构成的，今后讨论的模(module)与代数(algebra)所研究的对象除了集 M 上的代数运算外，还牵涉到**算子集**(operator set) R 对基集 M 的算子乘法(或数量乘法、倍数乘法). 其实模就是向量空间概念的推广，它牵涉到群、环、向量空间三种代数结构，它的内涵十分丰富. 我们将重点介绍主理想整环 D 上的模的性质和应用.

16.1 定义及例子

定义 16.1.1 设 $\langle R;+,\cdot\rangle$ 是有单元 1 的环，$\langle M;+\rangle$ 是加群，在 R 与 M 间规定一个 $R\times M$ 到 M 的称为算子乘法的代数运算"·"

$$(a,x)\mapsto a\cdot x,\quad a\in R,\quad x\in M,\quad a\cdot x\in M,$$

并满足下列条件：

(1) $a\cdot(x+y)=a\cdot x+a\cdot y,\quad a\in R,\quad x,y\in M;$

(2) $(a+b)\cdot x=a\cdot x+b\cdot x,\quad a,b\in R,\quad x\in M;$

(3) $(ab)\cdot x=a\cdot(bx),\quad a,b\in R,\quad x\in M;$

(4) $1\cdot x=x.$

则加群 M 叫做环 R 上的一个**左模**(left module)或**左 R-模**.

同样可以定义环 R 上的**右模**(right module)或**右 R-模**，这只要规定一个 $M\times R$ 到 M 的"右乘"运算"$*$"

$$(x,a)\mapsto x*a,$$

并满足下列条件：

(1) $(x+y)*a=x*a+y*a$, $a\in R$, $x,y\in M$;

(2) $x*(a+b)=x*a+y*b$, $a,b\in R$, $x\in M$;

(3) $x*(ab)=(x*a)*b$. $a,b\in R$, $x\in M$;

(4) $x*1=x$.

注 16.1.2 (1) 定义 16.1.1 中的左乘、右乘以及环 R 中的乘法本应该用不同的符号表示，但为了简便及避免混乱，我们将按照过去的做法把各种乘号全部省去.

(2) 由于左模及右模的定义是对偶的，它们有完全相似的结论，今后仅讨论左模并简称为模，读者不难将这些结论移植到右模上去.

(3) 定义**双模**(bi-module)如下：设 R,S 是两个有单元的环，若 M 既是左 R-模又是右 S-模，并且 $\forall r\in R, \forall s\in S, \forall m\in M$ 都有

$$(rm)s = r(ms),$$

则 M 叫做 R-S **双模**. 特别地，可以在交换环上定义双模.

例 16.1.3 (1) 设 $R=F$ 是域，$M=V$ 是 F 上的向量空间，R 在 M 上的运算是 F 的元对 V 中的向量作“数乘”，则 V 是左 F-模. 由于 F 的乘法是可交换的，则 V 又是右 F-模.

(2) 设 $R=\mathbf{Z}$ 是整数环，$M=G$ 是交换群，若群的运算为乘法，规定

$$na = \underbrace{a\cdot a\cdots a}_{n\text{个}} = a^n \qquad (n\in\mathbf{Z},\quad a\in G),$$

则 G 就是左 $\mathbf{Z}$-模；若 G 的运算为加法，则 $\mathbf{Z}$ 在 G 上的算子乘法实为求元 a 的倍元，即若 $n>0$，则 $n\cdot a=\underbrace{a+a+\cdots+a}_{n\text{个}}$，它当然也是左 $\mathbf{Z}$-模.

(3) 设 R 是有单元 1 的环，它对于加法构成一个加群 R_+. 若

规定 R 对 R_+ 的算子乘法 a_l 如下：

$$a_l(x) = ax, \qquad \forall a \in R, \forall x \in R_+,$$

则 R_+ 构成左 R-模；若规定 R 对 R_- 的算子乘法 a_r 为

$$a_r(x) = xa, \qquad \forall a \in R, \forall x \in R_+,$$

则 R_+ 构成右 R-模.

(4) 设 $M=V$ 为域 F 上的向量空间，A 为 V 的任一线性变换，$R=F[\lambda]$ 为 F 上的一元多项式环，λ 为 F 上的超越元(亦称未定元). 规定 $F[\lambda]$ 在 V 上的算子乘法为

$$f(\lambda) \cdot \alpha = f(A)(\alpha), \quad \alpha \in V,$$

则 V 是左 $F[\lambda]$-模. 这个模的结构完全由给定的线性变换 A 决定，此时 $f(\lambda)$ 对向量 α 的运算详细写出是：设 $f(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n$，$a_i \in F$，则 $f(A) = a_0E + a_1A + \cdots + a_nA^n$，$E$ 为单位变换，因而

$$f(\lambda) \cdot \alpha = f(A)(\alpha) = a_0\alpha + a_1A(\alpha) + \cdots + a_nA^n(\alpha).$$

定理 16.1.4 设 M 是一个 R-模，则下列运算规律成立：

(1) $a \cdot 0 = 0, a \cdot (-x) = -a \cdot x, a \in R, x \in M$;

(2) $0 \cdot x = 0, (-a) \cdot x = -a \cdot x, a \in R, x \in M$;

(3) $a \cdot \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} a \cdot x_i$; $(\sum_{i=1}^{n} a_i) \cdot x = \sum_{i=1}^{n} a_i \cdot x$.

16.2 子模与商模

定义 16.2.1 模 M 的一个非空子集 N 称作 M 的**子模**(submodule)，若它满足以下两个条件：

(1) N 为 M 的一个子群；

(2) 对 $\forall a \in R$, $\forall y \in N$ 都有 $ay \in N$.

显然 $\{0\}$ 和 M 本身都是 M 的子模，称为 M 的平凡子模.

例 16.2.2 (1) 向量空间 V 的每个子空间都是一个子模；反

之，向量空间 V 的每个子模也是它的子空间.

(2) 交换群 G 的每个子群 H 是 $\mathbf{Z}$-模 G 的一个子模，因为 $\forall n\in\mathbf{Z}$ 及 $\forall x\in H$ 都有 $nx=x^n\in H$.

(3) 环 R 的每个左理想(指 R 的关于加法和左乘法为封闭的集)都是模 R 的一个子模；反之，模 R 的每个子模都是环 R 的一个左理想.

(4) 设 V_1 是向量空间 V 的线性变换 A 的不变子空间，则 V_1 也是 $F[\lambda]$-模 V 的子模.

(5) 设 M_1 和 M_2 都是 R-模 M 的子模，令

$$M_1+M_2=\{m_1+m_2 \mid m_1\in M_1, m_2\in M_2\},$$

则 M_1+M_2 是 M 的一个子模，称为子模 M_1 与 M_2 的和.

(6) 一般地，设 $\{M_\lambda \mid \lambda\in\Gamma\}$ 是 R-模 M 的一簇子模，作

$$\sum_{\lambda\in\Gamma}M_\lambda=\Big\{\sum_{\lambda\in\Gamma}m_\lambda \,\Big|\, m_\lambda\in M_\lambda,\lambda\in\Gamma,\sum_{\lambda\in\Gamma}m_\lambda \text{ 中只有有限多项} \neq 0\Big\},$$

则 $\sum\limits_{\lambda\in\Gamma}M_\lambda$ 是 M 的子模.

(7) 设 $y_1,y_2,\cdots,y_r$ 是 R-模 M 的 r 个元，令

$$N=\Big\{\sum_{i=1}^{r}a_iy_i \,\Big|\, a_i\in R\Big\},$$

则 N 是 M 的一个子模，称为由 $y_1,y_2,\cdots,y_r$ 生成的子模，用

$$N=R(y_1,y_2,\cdots,y_r) \text{ 表示.}$$

(8) 模 M 的任意多个子模的交仍是 M 的子模.

定义 16.2.3 若模由有限多个元生成，则称 M 为**有限生成模**(finitely generated module)，这些元称为它的**生成元**(generator).

定义 16.2.4 设 N 是 R-模 M 的子模，则 N 是 M 的不变子群，而且商群 $\overline{M}=M/N$ 是交换群，若规定 R 的元 r 与 M/N 的元 $\overline{m}$ 的乘法为

$$r\cdot\overline{m}=\overline{rm},$$

则$\langle \overline{M}, +, \cdot \rangle$构成 R-模，称它为 R-模 M 关于子模 N 的**商模**(quotient module).

例 16.2.5 (1) 若 M 是 R-模，则 M/M 是零模.

(2) 整数环 $\mathbf{Z}$ 是 $\mathbf{Z}$-模，设 n 为一固定整数，则

$$(n) = \{kn \mid k \in \mathbf{Z}\}$$

是 $\mathbf{Z}$ 的一个子模，$\mathbf{Z}/(n)=\mathbf{Z}_n$ 是 $\mathbf{Z}$-模 $\mathbf{Z}$ 关于子模(n)的商模.

(3) 在例 16.2.2 中，设 N 为环 R 的左理想，则商群 R/N 是 R-模.

(4) 在例 16.2.2 中，设V_1是 V 的 A 的不变子空间，则商空间 V/V_1 是 $F[\lambda]$-模，而且 A 在商模中可诱导出线性变换.

16.3 模同态及基本定理

定义 16.3.1 设 M 和 M'是两个 R-模，若存在 M 到 M'的映射 η 满足：

(1) η 是群同态，

(2) $\eta(ax)=a\eta(x), \qquad \forall a \in R, \forall x \in M$,

则称 η 为 M 到 M'的**模同态**(module homomorphism)或 ***R*-同态**，用 $\mathrm{Hom}(M,M')$表示.

特别地，若 η 是 M 到 M' 的双射，则 η 叫做**模同构**(module isomorphism).

例 16.3.2 (1) 设 M,M'都是加群，于是它们都是 $\mathbf{Z}$-模，则 M 到 M'的群同态 η 必是 M 到 M'的一个 $\mathbf{Z}$-同态.

(2) 设 V 与 V'都是域 F 上的向量空间，则 V 到 V'的每个线性映射 φ 都是 V 到 V'的 F-同态. 特别地，当 $V=V'$时，V 的 F-自同态恰是 V 的线性变换.

(3) 令 $M=R^{(n)}=\{(x_1,x_2,\cdots,x_n) \mid x_i \in R\}$是环 R 上的模，则

$\varepsilon_i:(x_1,x_2,\cdots,x_i,\cdots,x_n) \mapsto x_i$

是 $R^{(n)}$ 到 R 的满同态，ε_i 称为在 x_i 轴上的射影，又设

$$\tau_i: x \mapsto (0, \cdots, 0, x, 0, \cdots, 0),$$

其中 x 在第 i 个位置上，则 τ_i 是 R 到 $R^{(n)}$ 的 R-单同态.

定义 16.3.3 设 M 与 M' 都是 R-模，$\eta: M \to M'$ 是 R-同态，则 $\eta(M)$ 称为 η 的**像**(image)，记作 $\mathrm{Im}\eta$；而 $\eta^{-1}(0')$ 称为 η 的**核**(kernel)，记作 $\ker\eta$. η 的像与核分别构成 M' 及 M 的子模.

像群和环的同态定理一样，也有模的几个同态定理.

定理 16.3.4 模同态基本定理 设 η 是 R-模 M 到 R-模 N 的 R-同态，则

$$M/\ker\eta \cong \mathrm{Im}\eta.$$

若将 R-模 $M/\ker\eta$ 称为 η 的**上像**(coimage)，并记之为 $\mathrm{Coim}\eta$，则此基本定理可改述为

$$\mathrm{Coim}\eta \cong \mathrm{Im}\eta.$$

定理 16.3.5 模同态对应定理 若 η 是 R-模 M 到 R-模 M' 的满同态，则 M 的包含 $\ker\eta$ 的子模的集 $S=\{N \mid \ker\sigma \subseteq N \subseteq M\}$ 与 M' 的子模集 $S'=\{\eta(N)\}$ 等势(即在 S 与 S' 间可建立双射).

定理 16.3.6 模同构定理

(1) 若 A 和 B 都是 R-模 M 的子模，则 $(A+B)/A \cong B/(A \cap B)$.

(2) 若 A 和 B 都是 R-模 M 的子模，且 $B \supseteq A$，则

$$M/B \cong (M/A)/(B/A).$$

定义 16.3.7 设 M 是 R-模，若它是由 M 的一个元 x 生成的(例 16.2.2)：

$$M = Rx = \{ax \mid a \in R\},$$

则称 M 为由元 x 生成的**循环 R-模**(cyclic R-module)，简称**循环模**，用 $M=Rx$ 表示.

例 16.3.8 (1) 每个循环群(a)都是一个循环 $\mathbf{Z}$-模.

(2) 每个有单元的环 R 都可看成一个 R-模，它也是循环 R-模，因为 $R=R \cdot 1$.

设 M 是 R-模，x 是 M 的一个元，作 M 到循环 R-模 Rx 的映射：

$$\eta_x: a \mapsto ax, \quad \forall a \in R,$$

则可证 η_x 是模 R 到 Rx 的一个模同态，而且它的核 $\ker\eta_x = \{a \in R \mid a \cdot x = 0\}$ 是 R 的一个左理想，根据同态基本定理有

$$Rx \cong R/\ker\eta_x.$$

定义 16.3.9 (1) 例 16.3.8(2)中 η_x 的核 $\ker\eta_x = \{a \in R \mid a \cdot x = 0\}$ 称为元 x 的**零化子**(annihilator)或元 x 的**阶理想**(order ideal)，记为 $\mathrm{ann}x$.

(2) 设 M 是一个 R-模，若规定

$$\mathrm{ann}(M) = \{a \in R \mid a \cdot x = 0 \quad \forall x \in M\},$$

则 $\mathrm{ann}(M)$ 是左理想也是右理想，称为 M 的零化子.

定理 16.3.10 (1) $Rx \cong R/\mathrm{ann}(x)$；

(2) $\mathrm{ann}(M) = \bigcap\limits_{x \in M} \mathrm{ann}(x)$；

(3) 若 R-模 M 不是零模，$x \neq 0$，则 R 的单元 1 必不属于 $\mathrm{ann}(x)$.

例 16.3.11 (1) 设 G 是一个交换群，则它可看作整数环 $\mathbf{Z}$ 上的一个模. 任取 $x \in G$，x 的零化子 $\mathrm{ann}(x)$ 是 $\mathbf{Z}$ 的一个理想，由于 $\mathbf{Z}$ 是主理想整环(定理 15.16.18)，可设 $\mathrm{ann}(x) = (n)$. 于是 $\langle x \rangle \cong \mathbf{Z}/(n)$. 当 $n = 0$ 时，$\langle x \rangle \cong \mathbf{Z}$，$\langle x \rangle$ 是无限循环群. 当 $n > 0$ 时，$\langle x \rangle$ 是 n 阶循环群，n 为元 x 的阶，而 (n) 是模元 x 的阶理想，故模元 x 的阶理想实为群元阶概念的推广.

(2) 设 V 是域 F 的 n 维向量空间，A 是一线性变换，则 V 是一个 $F[\lambda]$-模，$\forall x \in V$，$\lambda x = A(x)$. 现取一固定 x 作循环 $F[\lambda]$-子模 $V_1 = F[\lambda]x$，此时 $\mathrm{ann}(x)$ 是 $F[\lambda]$ 的一个主理想(定理 15.16.18)，设 $\mathrm{ann}(x) = (m(\lambda))$，其中 $m(\lambda)$ 是首项系数为 1 的多项式，它是由 x 唯一决定的，叫做 **x 的极小多项式**(minimum polynomial of x). 由零化子定义知，$f(\lambda)x = 0 \Leftrightarrow m(\lambda) \mid f(\lambda)$. 若

$x\neq 0$,则 $m(\lambda)$是一个正次数多项式;若$x=0$,则 $m(\lambda)=1$,$\mathrm{ann}(0)=F[\lambda]$.

16.4 加群上的及模上的自同态环

本节将在交换群及 R-模上考虑其自同态所组成的集,可以证明,它们对于所规定的运算都构成环,且对于任一给定的环总可以作一个自同态环与它同构.

定理 16.4.1 设 M 是加群,$\mathrm{End}M$ 是 M 的一切自同态所构成的集,在 $\mathrm{End}M$ 中规定乘法"·"及加法"+"($\forall \eta,\xi\in \mathrm{End}M$)如下:

$$(\eta\cdot\xi)(x)=\eta(\xi(x))\qquad(\forall x\in M),$$
$$(\eta+\xi)(x)=\eta(x)+\xi(x)\qquad(\forall x\in M),$$

则$\langle \mathrm{End}M;+,\cdot\rangle$构成环.

定义 16.4.2 定理 16.4.1 中的环$\langle \mathrm{End}M;+,\cdot\rangle$称为加群 M 的**自同态环**(ring of endomorphism).

例 16.4.3 (1) 设 M 是由元 a 生成的无限循环群 $M=(a)$,其运算为加法,则它的每个元 $b=na(n\in \mathbf{Z})$. 从而 M 上的每个自同态 η 由 a 的像唯一确定:

$$\eta(a)=za\qquad z\in\mathbf{Z}.$$

反之,可证此映射确是 M 的自同态. 用 η_z表示 M 的自同态,则

$$\mathrm{End}M=\{\eta_z\mid z\in\mathbf{Z}\}.$$

显然这个自同态环$\langle \mathrm{End}M;+,\cdot\rangle$与整数环$\langle \mathbf{Z};+,\cdot\rangle$同构,这只要在 $\mathbf{Z}$ 与 $\mathrm{End}M$ 间作映射 $z\mapsto\eta_z$就可以看出. 因此可以说,任一无限循环群的自同态环是整数环 $\mathbf{Z}$.

(2) 设 M_n是 n 阶加法循环群:$M_n=(a)$,仿上可以建立 $\mathbf{Z}$ 到 $\mathrm{End}M_n$ 的满同态:$z\rightarrow\eta_z$使得 $\eta_z(a)=za$, 此时同态的核不再是(0)

而是(n)，所以

$$\mathrm{End}M_n \cong \mathbf{Z}_n.$$

定理 16.4.4 设R是有单元1的环，则R同构于加群的自同态环.

在加群的自同态环的基础上可以类似地建立模的自同态环.

定义 16.4.5 设M是一个R-模，它上面的所有模自同态构成的集$\mathrm{Hom}(M,M)$关于所规定的"+"与"·"构成一个环，该环称为R-模M的自同态环，用$\mathrm{End}_R M$表示.

例 16.4.6 (1) 加群G作为$\mathbf{Z}$-模的自同态环就是群G的自同态环.

(2) 域F上的向量空间V是一个F-模. V的每个F-自同态η是一个线性变换；反之亦然. 所以V的自同态环就是由全部线性变换组成的环.

16.5 自由模

环R上的自由模是域上的向量空间概念的推广，为此也像线性代数一样要引入线性关系、线性无关、基等概念，可以看出向量空间的某些性质可以移植到自由R-模上去.

16.5.1 定义和性质

定义 16.5.1 设R是有单元的环，M是R-模.

(1) $S_1=\{x_1,\cdots,x_r\}$是M的有限子集，若它的任一线性关系

$$a_1x_1+\cdots+a_rx_r \qquad (a_i\in R)$$

仅在$a_1=\cdots=a_r=0$时才等于0，则称S_1为**R-线性无关的**(R-linear independence).

(2) 设S是模M的一个非空子集，若它的每个有限子集都是R-线性无关的，则称S是R-线性无关的.

定义 16.5.2 设 S 是模 M 的一组生成元(定义 16.2.3),且 S 是 R-线性无关的,则 S 称作 M 的**基**(base)与向量空间的基一样,有以下定理.

定理 16.5.3 设 S 是模 M 的基,则 M 的每个元用这个基表示的表达式是唯一的,即若 $a\in M$,有

$$\sum_{x\in S}a_x x = \sum_{x\in S}b_x x,$$

则 $a_x=b_x \quad (\forall x\in S)$.

定义 16.5.4 若 R-模 M 有基,则 M 称作**自由 R-模**(free R-module).

例 16.5.5 环 R 的积集 $R^{(n)}$ 构成的自由模:设 R 是有单元的环,作积集 $R^{(n)}=\{(x_1,\cdots,x_n)\mid x_i\in R\}$,并规定 $R^{(n)}$ 中元的相等、加法和 R 对 $R^{(n)}$ 的乘法如下:

$$(x_1,x_2,\cdots,x_n)=(y_1,y_2,\cdots,y_n)\Leftrightarrow x_i=y_i,$$
$$i=1,2,\cdots,n;$$
$$(x_1,x_2,\cdots,x_n)+(y_1,y_2,\cdots,y_n)$$
$$=(x_1+y_1,x_2+y_2,\cdots,x_n+y_n);$$
$$a\cdot(x_1,x_2,\cdots,x_n)=(a\cdot x_1,a\cdot x_2,\cdots,a\cdot x_n),a_i\in R.$$

则 $R^{(n)}$ 是 R-模,其零元 $\mathbf{0}=(0,0,\cdots,0)$,$(x_1,x_2,\cdots,x_n)$ 的反元是 $(-x_1,-x_2,\cdots,-x_n)$. 令 $\boldsymbol{e}_1=(1,0,\cdots,0)$,$\boldsymbol{e}_2=(0,1,0,\cdots,0)$,$\cdots$,$\boldsymbol{e}_n=(0,\cdots,0,1)$,则集$\{\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_n\}$是 $R^{(n)}$ 的基,因此 $R^{(n)}$ 是自由模.

与 n 维向量空间中 $F^{(n)}$ 的作用一样,本例的自由模在模论中占有重要地位.

定理 16.5.6 设 M 是自由 R-模,$\{u_1,u_2,\cdots,u_n\}$ 是它的基;又设 M' 是任一 R-模,$\{v_1,v_2,\cdots,v_n\}$ 是 M' 的任一子集,则映射

$$\eta: u_i\mapsto v_i,$$

必可唯一地扩张成 M 到 M' 的一个 R-同态 η'.

定理 16.5.7 设 M 是以 $\{u_1, u_2, \cdots, u_n\}$ 为基的自由 R-模，则 $M \cong R^{(n)}$.

定理 16.5.8 设 M 是自由 R-模，$\{x_1, x_2, \cdots, x_r\}$ 是它的基，I 是 R 的理想，作 $N = Ix_1 + Ix_2 + \cdots + Ix_r$，则商模 M/N 可看作 $\overline{R}(=R/I)$-模，而且 M/N 是 $\overline{R}$ 上的一个自由模，$\{\overline{x_i} = x_i + N \mid i = 1, 2, \cdots, r\}$ 是它的基.

定理 16.5.9 设 R 是有单元 1 的交换环，M 是自由 R-模，则 M 的任意两组基的个数相等，即 M 的基的个数是一个不变量.

定理 16.5.10 设 R 是有单元 1 的交换环，若 $R^{(m)}$ 与 $R^{(n)}$ 是模同构，则 $m=n$.

定义 16.5.11 设 R 是有单元 1 的交换环，M 是自由 R-模，它的任一基的个数称为该模的**秩**(rank).

定理 16.5.12 给定有单元 1 的交换环 R 和一个正整数 n，恰有一个(在模同构的意义下)秩为 n 的自由 R-模. 且如果两个模的秩不相等，则它们必不模同构. 因此自由 R-模的构造完全由模的秩所决定.

例 16.5.13 (1) 设 $R = \mathbf{Z}/(6) = \mathbf{Z}_6 = \{[0], [1], \cdots, [5]\}$. $R^{(2)}$ 是秩为 2 的自由 R-模，$\boldsymbol{e}_1 = ([1], [0])$ 和 $\boldsymbol{e}_2 = ([0], [1])$ 是 $R^{(2)}$ 的一组基. 这个模的有些元是线性无关的(如 $\boldsymbol{x} = [2]\boldsymbol{e}_1 + [3]\boldsymbol{e}_2$)，但 $\boldsymbol{y} = [2]\boldsymbol{e}_1 + [2]\boldsymbol{e}_2$ 却是线性相关的，因为$[3] \neq [0]$，但$[3] \cdot \boldsymbol{y} = \boldsymbol{0}$.

(2) 设 $R = \mathbf{Z}, M = \mathbf{Z}^{(2)}$，则 $\boldsymbol{e}_1 = (1,0)$，$\boldsymbol{e}_2 = (0,1)$ 是 M 的一组基，故 M 的秩是 2. 再看由 $\boldsymbol{x}_1 = 2\boldsymbol{e}_1$ 及 $\boldsymbol{x}_2 = 3\boldsymbol{e}_2$ 在 M 中生成的子模 N，显然它是 M 的一个自由 R-真子模，而且 $\boldsymbol{x}_1, \boldsymbol{x}_2$ 是它的一组基，故 N 的秩亦为 2.

本例说明模与它的真子模可以有相同的秩，这与向量空间的情况不同.

16.5.2 自由模的同态与矩阵

在自由模中可以利用矩阵来研究 $R^{(m)}$ 到 $R^{(n)}$ 内的模同态 $\mathrm{Hom}(R^{(m)},R^{(n)})$.

定义 16.5.14 在 $R^{(m)}$ 与 $R^{(n)}$ 内各取基 $\{\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_m\}$ 及 $\{\boldsymbol{f}_1,\boldsymbol{f}_2,\cdots,\boldsymbol{f}_n\}$，设 $\eta\in\mathrm{Hom}(R^{(m)},R^{(n)})$，而且

$$\eta(\boldsymbol{e}_1)=a_{11}\boldsymbol{f}_1+a_{12}\boldsymbol{f}_2+\cdots+a_{1n}\boldsymbol{f}_n,$$
$$\eta(\boldsymbol{e}_2)=a_{21}\boldsymbol{f}_1+a_{22}\boldsymbol{f}_2+\cdots+a_{2n}\boldsymbol{f}_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\eta(\boldsymbol{e}_m)=a_{m1}\boldsymbol{f}_1+a_{m2}\boldsymbol{f}_2+\cdots+a_{mn}\boldsymbol{f}_n.$$

则 $m\times n$ 矩阵 $\boldsymbol{A}=(a_{ij})$ 称为 **$\boldsymbol{\eta}$ 关于基 $\{\boldsymbol{e}_i\}$，$\{\boldsymbol{f}_j\}$ 的矩阵**.

定理 16.5.15 同态映射 η 完全由矩阵 $\boldsymbol{A}$ 确定. 若设

$$\boldsymbol{x}=(x_1,x_2,\cdots,x_m)=\sum_i x_i\boldsymbol{e}_i,$$
$$\boldsymbol{y}=(y_1,y_2,\cdots,y_n)=\sum_j y_j\boldsymbol{f}_j,$$
$$\eta:(x_1,x_2,\cdots,x_m)\mapsto(y_1,y_2,\cdots,y_n),$$

则

$$(y_1,y_2,\cdots,y_n)=(x_1,x_2,\cdots,x_m)\boldsymbol{A}.$$

定理 16.5.16 用 $M_{m,n}(R)$ 表示 R 上的 $m\times n$ 矩阵的集，规定 $M_{m,n}(R)$ 中两矩阵 $\boldsymbol{A}=(a_{ij})$ 与 $\boldsymbol{B}=(b_{ij})$ 的和为

$$\boldsymbol{A}+\boldsymbol{B}=(a_{ij})+(b_{ij})=(a_{ij}+b_{ij}),$$

则 $\langle M_{m,n}(R);+\rangle$ 是加群，且此群同构于 $\mathrm{Hom}(R^{(m)},R^{(n)})$.

进而可以规定矩阵的乘法，并可证明矩阵乘法(在可乘的前提下)满足结合律及乘法关于加法的两个分配律，从而有以下定理.

定理 16.5.17 作 $R^{(n)}$ 的自同态环 $\mathrm{End}_R R^{(n)}=\mathrm{Hom}(R^{(m)},R^{(n)})$ 到 n 阶矩阵集 $M_n(R)$ 的映射

$$\varphi:\eta\mapsto\boldsymbol{A}.$$

则 φ 是一个能保持加法和乘法及其一切运算规律的双射，因而 φ 是环同构，从而 $M_n(R)$ 构成一个有单元的环，其单元是单位矩阵，

它与 $\mathrm{End}_R R^{(n)}$ 的恒等映射相对应.

高等代数里建立的 n 阶行列式理论亦可类似地推广到交换环 R 上的 $n\times n$ 矩阵环 $M_n(R)$ 中去,而且大多数性质都能继续成立.

16.6 模的直和

如同研究其他代数结构一样,我们在研究模时也常将它分解成一些互不相交的子模的"直和".

定义 16.6.1 设 $M_1,M_2,\cdots,M_n$ 是同一个环 R 上的 n 个模,作积集

$$M=M_1\times M_2\times\cdots\times M_n=\{(x_1,x_2,\cdots,x_n)\mid x_i\in M_i\},$$

仿例 16.5.5 规定 M 内的加法、零元及用 R 的元乘 M 的元的乘法后,所得的模 $\langle M;+,\cdot,0\rangle$ 称为各模 M_i 的**直和**(direct sum),用 $M_1\oplus M_2\oplus\cdots\oplus M_n$ 或 $\oplus M_i$ 表示.

定理 16.6.2 设 M 是模,它所包含的子模 $M_1,M_2,\cdots,M_n$ 具有以下性质:

(1) $M=M_1+M_2+\cdots+M_n$(即 M 由各 M_i 生成);

(2) $\forall i\in\{1,\cdots,n\}$,有

$$M_i\cap(M_1+\cdots+M_{i-1}+M_{i+1}+\cdots+M_n)=\{0\},$$

则映射 $\eta:(x_1,x_2,\cdots,x_n)\mapsto\sum_{i=1}^{n}x_i$ 是 $\oplus M_i$ 到 M 的一个同构;反之,在 $\oplus M_i$ 中,若令 $M_i'=\{(0,\cdots,0,x_i,0,\cdots,0)\mid x_i\in M_i\}$,则 M_i' 是直和 $\oplus M_i$ 的同构于 M_i 的子模,而且 $\oplus M_i$ 的这些子模满足条件(1),(2).

该定理容许在 M 的子模 M_i 满足条件(1)、(2)下将模 M 与直和 $\oplus M_i$ 等同看待.

定义 16.6.3 设 $M_1,M_2,\cdots,M_n$ 是模 M 的子模,若它们能满

足定理 16.6.2 的条件，则 M 称为各 M_i 的**内直和**(internal direct sum)或**直和**(direct sum)，记为 $M=\bigoplus M_i$ 或 $M=M_1\oplus M_2\oplus\cdots\oplus M_n$.

定义 16.6.4 若模 M 的子模 $M_1, M_2, \cdots, M_n$ 满足定理 16.6.2 中的条件(2)，则称这些子模是**独立的**(independent).

注意：条件(2)与条件 $M_i\cap M_j=\{0\}(i\neq j)$ 是有区别的，使用时要小心.

定理 16.6.5 (1) 设 $M_1, \cdots, M_n$ 是模 M 的独立子模，作和 $N_1=M_1+\cdots+M_{r_1}$, $N_2=M_{r_1+1}+\cdots+M_{r_1+r_2}$, $N_3=M_{r_1+r_2+1}+\cdots+M_{r_1+r_2+r_3}$, $\cdots$，则这些和 $N_1, N_2, N_3, \cdots$ 也是独立的.

(2) 设 $M_1, \cdots, M_n$ 是独立的，且设 $M_i=M_{i1}\oplus M_{i2}\oplus\cdots\oplus M_{ir_i}$, $1\leqslant i\leqslant n$，其中 M_{ij} 都是 M_i 的子模，则诸子模 $M_{11}, \cdots, M_{1r_1}$, $M_{21}, \cdots, M_{2r_2}, \cdots, M_{n1}, \cdots, M_{nr_n}$ 也是独立的.

定理 16.6.6 (1) 设 $M=\bigoplus M_i$, M_i 是 M 的子模，令 $N_1=M_1+\cdots+M_{r_1}$, $N_2=M_{r_1+1}+\cdots+M_{r_1+r_2}$, $\cdots$. 则 $M=\bigoplus N_j$.（即：若模 M 是各子模 M_i 的直和，则 M 也是这些子模 M_i 组成的部分和 N_j 的直和.）

(2) 若 $M_i=\bigoplus M_{ij}$, $1\leqslant i\leqslant n$, $1\leqslant j\leqslant r_i$，则 $M=\bigoplus M_{ij}$.（即若 M_{ij} 所组成的各部分和是直和，则 M_{ij} 的总和 M 也是直和）.

此定理是定理 16.6.5 的推论.

16.7 主理想整环上的有限生成模

在 15.16.2 节中已介绍过主理想整环，它是有单元 1 的交换整环，它的每个理想都是主理想，可以证明它是唯一分解整环，它有一些性质是一般环所不具有的，本节将专门介绍其上的有限生成模. 可以发现域上向量空间的某些性质在其上也能成立.

16.7.1 初步结果

定理 16.7.1 设 M 是主理想整环 D 上的秩为 m 的自由 D-模，则 M 的任一子模 N 也是自由 D-模，且 N 的秩 $n\leqslant m$.

定理 16.7.2 设 D 是主理想整环，M 是由有限集 $\{x_1, x_2, \cdots, x_m\}$ 生成的 D-模：

$$M=\sum_{i=1}^{m} Dx_i,$$

作 $D^{(m)}$ 到 M 的映射

$$\eta: \sum_{i=1}^{m} a_i\boldsymbol{e}_i \mapsto \sum_{i=1}^{m} a_i x_i,$$

则 η 是 $D^{(m)}$ 到 M 的同态满射，且

$$M\cong D^{(m)}/K,$$

其中 $K=\ker\eta$ 是 $D^{(m)}$ 的子模，此子模是自由的且其基的个数 $k\leqslant m$.

例 16.7.3 (1) 任意域 F 都是主理想整环(因域仅有(0)和(1)两个理想)，因而域 F 上的 n 维向量空间 V 是主理想整环 F 上的一个自由的、秩为 n 的有限生成模；由定理 16.7.1 可知，它的任一子空间都是有限维的且其维数 $s\leqslant n$.

(2) 在例 16.5.13(2) 中，由于 $R=\mathbf{Z}$ 是欧氏整环(定义 15.16.17)，所以它是主理想整环，$M=\mathbf{Z}^{(2)}$ 是秩为 2 的自由 $\mathbf{Z}$-模，其真子模 N 的秩亦为 2.

(3) 注意：若 R 不是主理想整环，则 R-自由模的子模不一定是自由的，例如 $R=\mathbf{Z}_6$，则 $M=R^{(2)}$ 是一个秩为 2 的自由 R-模，$\boldsymbol{e}_1=([1],[0])$ 及 $\boldsymbol{e}_2=([0],[1])$ 是 $R^{(2)}$ 的一组基；但由其元 $\boldsymbol{y}=[2]\boldsymbol{e}_1+[2]\boldsymbol{e}_2$ 生成的子模 $N=\{[0],\boldsymbol{y},2\boldsymbol{y}\}$ 却不是自由 R-模，因为它的每个子集都是线性相关的，所以没有基.

16.7.2 主理想整环上矩阵的等价

本节将在主理想整环上讨论把一个表示一组生成元与基的关系的矩阵简化成正规矩阵的问题.

设$\{\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_n\}$是子模 K 的生成元集，它用 $D^{(m)}$ 的基$\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_m\}$表示如下：

$\boldsymbol{f}_1 = a_{11}\boldsymbol{e}_1 + a_{12}\boldsymbol{e}_2 + \cdots + a_{1m}\boldsymbol{e}_m$,

$\boldsymbol{f}_2 = a_{21}\boldsymbol{e}_1 + a_{22}\boldsymbol{e}_2 + \cdots + a_{2m}\boldsymbol{e}_m$,

……………………

$\boldsymbol{f}_n = a_{n1}\boldsymbol{e}_1 + a_{n2}\boldsymbol{e}_2 + \cdots + a_{nm}\boldsymbol{e}_m$.

定义 16.7.4 用以上方程组的系数为元素的 D 上的 $n \times m$ 矩阵$\boldsymbol{A} = (a_{ki})$，称为生成元集$\{\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_n\}$用基$\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_m\}$表示的**关系矩阵**(relation matrix).

也可以另取 $D^{(m)}$ 的新基$\{\boldsymbol{e}'_1, \boldsymbol{e}'_2, \cdots, \boldsymbol{e}'_m\}$，设在新基$\{\boldsymbol{e}'_i\}$与旧基$\{\boldsymbol{e}_j\}$之间存在如下关系：

$$\boldsymbol{e}'_i = \sum_{j=1}^{m} p_{ij}\boldsymbol{e}_j,$$

其系数构成的矩阵 $\boldsymbol{P} = (p_{ij})$ 是矩阵环 $M_m(D)$ 的一个可逆矩阵. 此外设$\boldsymbol{Q} = (q_{kl})$是$M_n(D)$的一个可逆矩阵，其逆为$\boldsymbol{Q}^{-1} = (q^*_{kl})$，作元 $\boldsymbol{f}'_k = \sum\limits_{l=1}^{n} q_{kl}\boldsymbol{f}_l (k = 1, 2, \cdots, n)$，则可证$\{\boldsymbol{f}_i'\}$构成 K 的一个新生成元集，这时$\{\boldsymbol{f}_i'\}$与$\{\boldsymbol{e}'_i\}$间有如下关系

$$\boldsymbol{f}'_k = \sum q_{kl}\boldsymbol{f}_l = \sum_{l,j} q_{kl}a_{lj}\boldsymbol{e}_j = \sum_{l,j,i} q_{kl}a_{lj}p^*_{ji}\boldsymbol{e}'_i,$$

这里的$(p^*_{ij}) = \boldsymbol{P}^{-1}$. 因而有以下定理.

定理 16.7.5 在上述条件下，K 的新生成元集$\{\boldsymbol{f}'_i\}$用 $D^{(m)}$ 的新基$\{\boldsymbol{e}'_i\}$表示的关系矩阵是

$$\boldsymbol{A}' = (a'_{ki}) = \boldsymbol{QAP}^{-1}.$$

定义 16.7.6 设主理想整环 D 上的两个 $n \times m$ 矩阵 $\boldsymbol{A}_{n\times m}$ 及

$\boldsymbol{B}_{n\times m}$，若在 $M_n(D)$ 中存在一个可逆矩阵 $\boldsymbol{P}_n$，在 $M_m(D)$ 中存在一个可逆矩阵 $\boldsymbol{Q}_m$ 使得 $\boldsymbol{A}_{n\times m}=\boldsymbol{P}_n\boldsymbol{B}_{n\times m}\boldsymbol{Q}_m$，则称 $\boldsymbol{A}_{n\times m}$ 与 $\boldsymbol{B}_{n\times m}$ 是**等价矩阵**(equivalent matrix).

在线性代数中，域 F 上的 $n\times m$ 矩阵都可经过若干初等变换将它转化成与原矩阵等价的形式简单的"正规矩阵". 在主理想整环 D 上，也是如此，尽管化简法不尽相同.

定理 16.7.7 设 D 是主理想整环，$\mathbf{A}\in M_{n\times m}(D)$，则 $\mathbf{A}$ 必等价于下列对角形矩阵：

$$\operatorname{diag}(d_1,d_2,\cdots,d_r,0,\cdots,0)$$
$$=\begin{bmatrix} d_1 & & & & & 0 \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \\ 0 & & & & & 0 \end{bmatrix},$$

其中 $d_i\neq 0$ 且 $d_i\mid d_j(i\leqslant j)$.

定义 16.7.8 定理 16.7.7 中与矩阵 $\mathbf{A}$ 等价的对角形矩阵称为 $\mathbf{A}$ 的**正规形**(normal form).

定义 16.7.9 矩阵 $\mathbf{A}$ 的正规形中，对角线上的各个元(d_1，d_2，$\cdots$，d_r)称为 $\mathbf{A}$ 的**不变因子**(invariant factor).

D 上矩阵 $\mathbf{A}$ 的正规形(在容许各不变因子相差一个单位的意义下)是唯一的.

例 16.7.10 (1) 整数矩阵

$$\mathbf{A}=\begin{bmatrix} 6 & 2 & 3 & 0 \\ 2 & 3 & -4 & 1 \\ -3 & 3 & 1 & 2 \\ -1 & 2 & -3 & 5 \end{bmatrix}$$

的正规矩阵可如下求得(所作的行、列变换分别标示在箭头的上方与下方，其中的罗马数字表示行、列的号数)：

$$\begin{bmatrix} 6 & 2 & 3 & 0 \\ 2 & 3 & -4 & 1 \\ -3 & 3 & 1 & 2 \\ -1 & 2 & -3 & 5 \end{bmatrix} \xrightarrow{\mathrm{I} \leftrightarrow \mathrm{IV}} \begin{bmatrix} 0 & 2 & 3 & 6 \\ 1 & 3 & -4 & 2 \\ 2 & 3 & 1 & -3 \\ 5 & 2 & -3 & -1 \end{bmatrix} \xrightarrow{\mathrm{I} \leftrightarrow \mathrm{II}} \begin{bmatrix} 1 & 3 & -4 & 2 \\ 0 & 2 & 3 & 6 \\ 2 & 3 & 1 & -3 \\ 5 & 2 & -3 & -1 \end{bmatrix}$$

$$\xrightarrow[\substack{-3\mathrm{I}+\mathrm{II} \\ 4\mathrm{I}+\mathrm{III} \\ -2\mathrm{I}+\mathrm{IV}}]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 3 & 6 \\ 2 & -3 & 9 & -7 \\ 5 & -13 & 17 & -11 \end{bmatrix} \xrightarrow{\substack{-2\mathrm{I}+\mathrm{III} \\ -5\mathrm{I}+\mathrm{IV}}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 3 & 6 \\ 0 & -3 & 9 & -7 \\ 0 & -13 & 17 & -11 \end{bmatrix}$$

$$\xrightarrow[\mathrm{III}-\mathrm{II}]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 6 \\ 0 & -3 & 12 & -7 \\ 0 & -13 & 30 & -11 \end{bmatrix} \xrightarrow[\mathrm{II} \leftrightarrow \mathrm{III}]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 6 \\ 0 & 12 & -3 & -7 \\ 0 & 30 & -13 & -11 \end{bmatrix}$$

$$\xrightarrow[\substack{-2\mathrm{II}+\mathrm{III} \\ -6\mathrm{II}+\mathrm{IV}}]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 12 & -27 & -79 \\ 0 & 30 & -73 & -191 \end{bmatrix} \xrightarrow{\substack{-12\mathrm{II}+\mathrm{III} \\ -30\mathrm{II}+\mathrm{IV}}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -27 & -79 \\ 0 & 0 & -73 & -191 \end{bmatrix}$$

$$\xrightarrow[-3\mathrm{III}+\mathrm{IV}]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -27 & 2 \\ 0 & 0 & -73 & 28 \end{bmatrix} \xrightarrow[14\mathrm{IV}+\mathrm{III}]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 319 & 28 \end{bmatrix}$$

$$\xrightarrow[-2\mathrm{III}+\mathrm{IV}]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 319 & -610 \end{bmatrix} \xrightarrow{-319\mathrm{III}+\mathrm{IV}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -610 \end{bmatrix}$$

$$\xrightarrow{-1\mathrm{IV}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 610 \end{bmatrix}.$$

最后的矩阵即为 $\boldsymbol{A}$ 的正规矩阵.

(2) $M_3(\boldsymbol{Q}[\lambda])$ 里的矩阵 $\begin{bmatrix} \lambda+1 & 2 & -6 \\ 1 & \lambda & -3 \\ 1 & 1 & \lambda-4 \end{bmatrix}$ 的正规形是

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda-1 & 0 \\ 0 & 0 & (\lambda-1)^2 \end{bmatrix}.$$

16.7.3 主理想整环上有限生成模的构造定理

定理 16.7.11 基本定理 若 $M(\neq 0)$ 是主理想整环 D 上的有限生成模，则 M 是各循环模 Dz_i 的直和：

$M = Dz_1 \oplus Dz_2 \oplus \cdots \oplus Dz_s$,

各循环模的生成元 $z_1, z_2, \cdots, z_s$ 的序理想 $\mathrm{ann} z_i$ 满足条件：

$$\mathrm{ann} z_1 \supset \mathrm{ann} z_2 \supset \cdots \supset \mathrm{ann} z_s, \text{且 } \mathrm{ann} z_k \neq D.$$

例 16.7.12 (1) 设主理想整环 D 上的模 $M \cong \mathbf{Z}^{(3)}/K$，其中 K 是由 $\boldsymbol{f}_1 = (2,1,-3)$ 及 $\boldsymbol{f}_2 = (1,-1,2)$ 生成的，求 M 的构造. 此时 $\boldsymbol{f}_1, \boldsymbol{f}_2$ 关于 $\mathbf{Z}^{(3)}$ 的基 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$ 的关系矩阵是

$$\boldsymbol{A} = \begin{bmatrix} 2 & 1 & -3 \\ 1 & -1 & 2 \end{bmatrix},$$

令

$$\boldsymbol{Q} = \begin{bmatrix} 0 & 1 \\ -1 & 2 \end{bmatrix}, \boldsymbol{P} = \begin{bmatrix} 1 & -1 & 2 \\ 0 & -3 & 7 \\ 0 & 1 & -2 \end{bmatrix},$$

则

$$\boldsymbol{QAP}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

所以 $\boldsymbol{e}_1' = (1,-1,2)$, $\boldsymbol{e}_2' = (0,-3,7)$, $\boldsymbol{e}_3' = (0,1,-2)$；而 $\boldsymbol{f}_1' = \boldsymbol{e}_1'$, $\boldsymbol{f}_2 = \boldsymbol{e}_2'$. 故若取 $\{\boldsymbol{e}_1', \boldsymbol{e}_2', \boldsymbol{e}_3'\}$ 为 $\mathbf{Z}^{(3)}$ 的基时，K 由 $\{\boldsymbol{e}_1', \boldsymbol{e}_2'\}$ 生成，而

$$\mathbf{Z}^{(3)}/K=\mathbf{Z}e_3'\cong\mathbf{Z}.$$

因而 M 是与 $\mathbf{Z}$ 同构的模.

(2) 设 D 是 Gauss 整数环 $\mathbf{Z}[\sqrt{-1}]$,K 是由 $\boldsymbol{f}_1=(1,3,6)$,$\boldsymbol{f}_2=(2+3\mathrm{i},-3\mathrm{i},12-18\mathrm{i})$ 及 $\boldsymbol{f}_3=(2-3\mathrm{i},6+9\mathrm{i},-18\mathrm{i})$ 生成的,这里 $\mathrm{i}=\sqrt{-1}$. 则 $D^{(3)}/K$ 的构造可如下决定:

$\boldsymbol{f}_1,\boldsymbol{f}_2,\boldsymbol{f}_3$ 关于 $D^{(3)}$ 的基 $\{\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3\}$ 的关系矩阵是:

$$\boldsymbol{A}=\begin{bmatrix}1 & 3 & 6\\ 2+3\mathrm{i} & -3\mathrm{i} & 12-18\mathrm{i}\\ 2-3\mathrm{i} & 6+9\mathrm{i} & -18\mathrm{i}\end{bmatrix},$$

$$\boldsymbol{QAP}^{-1}=\begin{bmatrix}1 & & 0\\ & 6 & \\ 0 & & 24+96\mathrm{i}\end{bmatrix}.$$

于是 $D^{(3)}/K=Dz_1\oplus Dz_2$,这里生成元 z_1,z_2 的零化子分别是 $\mathrm{ann}z_1=(6)$,$\mathrm{ann}z_2=(24+96\mathrm{i})$.

16.7.4 扭模、准素分量与不变性定理

一般来说,主理想整环上有限生成模的分解未必是唯一的,这由构造最简单的自由模 $D^{(n)}$ 既可用 $\{\boldsymbol{e}_i\}$ 表成 $D^{(n)}=D\boldsymbol{e}_1\oplus\cdots\oplus D\boldsymbol{e}_n$(其中 $\mathrm{ann}\boldsymbol{e}_i=0$),又可利用其他的 $\{\boldsymbol{f}_i\}$(最简单的例如变更 $\{\boldsymbol{e}_i\}$ 的顺序及倍数等等)表成另一种形式的直和可见. 尽管如此,在这些表示式中还有不变的东西,本节将加以研究,为此需先引入扭子模的概念并探讨它的一些性质.

定义 16.7.13 设 x 是 D-模 M 的一个元,若有 $a(\neq 0)\in D$ 使 $ax=0$,则称 x 是 M 的一个**扭元**(torsion);若不存在 D 中的非零元 a 使 $ax=0$,则称 x 是 M 的一个**自由元**(free element).

例 16.7.14 (1) 交换群作为 $\mathbf{Z}$-模,它的扭元就是它的有限阶元.

(2) 设 V 是域 F 上的向量空间,它的每个非零元 $\boldsymbol{x}$ 都是自由

元，因为 $\forall a(\neq 0)\in F$ 都有 $a\cdot \boldsymbol{x}\neq \boldsymbol{0}$.

(3) 设 V 是域 F 上的 n 维向量空间，$\boldsymbol{A}$ 是一个线性变换，定义 $\lambda\boldsymbol{\alpha}=\boldsymbol{A}\boldsymbol{\alpha}$，则 V 是一元多项式环 $F[\lambda]$ 上的模，它的每个元 $\boldsymbol{\alpha}$ 都是扭元，这是因为 V 是 n 维向量空间，它的每个元都适合次数不超过 n 的方程 $f(\lambda)(\boldsymbol{\alpha})=0$.

定义 16.7.15 设 M 是 D-模，若 M 中的每个元都是扭元，则称 M 为**扭模**(torsion module)；若 M 中的每个元都是自由元，则称 M 为**无扭模**(untorsion module).

显然例 16.7.14(2) 中的 V 是无扭模，而例 16.7.14(3) 中的 $F[\lambda]$-V 是扭模.

定理 16.7.16 设 M 是主理想整环 D 上的有限生成模 $\mathrm{tor}M$ 是 M 的一切扭元所成的集：

$$\mathrm{tor}M=\{y\mid y\in M;\ \exists a(\neq 0)\in D \text{ 使 } a\cdot y=0\},$$

则 $\mathrm{tor}M$ 构成 M 的一个子模.

定理 16.7.17 主理想整环 D 上的任一有限生成模 M 都是它的扭子模与一个自由子模的直和.

为了将各扭模作更深入的解剖，现将对它所对应的序理想的生成元 d_i 作素因子分解：$d_i=p_1^{e_{1i}}p_2^{e_{2i}}\cdots p_k^{e_{ki}}$，因而有以下概念及性质.

定义 16.7.18 设 p 是主理想整环 D 的一个素元，模 M 中能使 $p^k y=0$ 对某个 $k\in\mathbf{N}$ 成立的元素 y 的子集称为 M 的 **p-分量**(p-component)，用 M_p 表示.

定理 16.7.19 (1) 每个 p-分量都是 M 的一个子模，它包含于 $\mathrm{tor}M$ 之中.

(2) 设 $p_1,p_2,\cdots,p_h$ 是 D 的不同的素元，它们的对应 p_i-分量必是独立的(见定义 16.6.4).

定义 16.7.20 如果一个循环模 Dx 的序理想 $\mathrm{ann}x=(p^e)$(p 是素元)，则称该模为**准素循环模**(primary cyclic module).

将循环模分解或合成时，它们的序理想有以下关系，这些关系式是将扭模分解或合成的依据.

定理 16.7.21 (1) 若 $M=Dx$，其中 $\operatorname{ann}x=(d)$ 且 $d=gh$，$(g,h)=1$，则 $M=Dy\oplus Dz$，其中 $\operatorname{ann}y=(g)$，$\operatorname{ann}z=(h)$.

(2) 若 $M=Dy\oplus Dz$，其中 $\operatorname{ann}y=(g)$，$\operatorname{ann}z=(h)$ 而且 $(g,h)=1$，则 $M=Dx$，其中 $\operatorname{ann}x=(gh)$.

因为 D 是主理想整环，它的每个元 $d(\neq\epsilon)$ 在容许相差一个单位的意义下都可作唯一分解(定义 15.16.1)：

$$d=p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t},$$

其中 p_i 为素元. 运用数学归纳法即可得

$$M=Dx_1\oplus Dx_2\oplus\cdots\oplus Dx_t.$$

这里的 $\operatorname{ann}x_i=(p_i^{e_i})$，因而将任一循环扭模分解成若干个准素循环模的直和.

定理 16.7.22 设 M 是主理想整环 D 上的有限生成扭模，则其准素分量 M_p 除对有限多个素数 $p_1,p_2,\cdots,p_h$ 不为零外，对几乎所有的 $M_p=0$，而且 $M=M_{p_1}\oplus M_{p_2}\oplus\cdots\oplus M_{p_h}$.

将基本定理中的循环扭模用准素循环扭模的直和表出即得如下定理.

定理 16.7.23 任一有限生成扭模都是准素循环模的直和.

例 16.7.24 由上可得到主理想整环上的有限生成扭模 M 的两种形式的直和分解：一种是 $M=Dz_1\oplus Dz_2\oplus\cdots\oplus Dz_r$，其中生成元 z_i 的阶理想成递降序列：

$$\operatorname{ann}z_1\supset\operatorname{ann}z_2\supset\cdots\supset\operatorname{ann}z_r(\neq 0).$$

若令 $\operatorname{ann}z_i=(d_i)$，则有 $d_i\mid d_{i+1}$.

另一种是

$$\begin{aligned}M=&Dx_{11}\oplus Dx_{12}\oplus\cdots\oplus Dx_{1h_1}\\&\oplus Dx_{21}\oplus Dx_{22}\oplus\cdots\oplus Dx_{2h_2}\end{aligned}$$

$$\oplus \cdots\cdots\cdots\cdots\cdots\cdots$$

$$\oplus Dx_{r1} \oplus Dx_{r2} \oplus \cdots \oplus Dx_{rh_r},$$

其中 Dx_{ij} 都是准素循环模，而且

$$\text{ann}x_{ij} = (p_j^{e_{ij}}), 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant h_i.$$

由定理 16.7.21 可知，扭模的这两种直和分解是可以互相转化的. 例如设有限 **Z**-模 M（实为有限交换群）的第二种直和分解是

$$M = \mathbf{Z}u_1 \oplus \mathbf{Z}u_2 \oplus \mathbf{Z}u_3 \oplus \mathbf{Z}v_1 \oplus \mathbf{Z}v_2 \oplus \mathbf{Z}w_1 \oplus \mathbf{Z}w_2.$$

其中

$$\text{ann}u_1 = (3^2), \text{ann}u_2 = (3^3), \text{ann}u_3 = (3^4);$$

$$\text{ann}v_1 = (5^2), \text{ann}v_2 = (5^4);$$

$$\text{ann}w_1 = (7), \text{ann}w_2 = (7^3).$$

这个有限模（有限交换群）的阶$=3^9 \cdot 5^6 \cdot 7^4$.

按定理 16.7.21(2)有

$$M = \mathbf{Z}x_1 \oplus \mathbf{Z}x_2 \oplus \mathbf{Z}x_3,$$

其中 $x_1 = u_1, x_2 = u_2 + v_1 + w_1, x_3 = u_3 + v_2 + w_2$. 并有

$\text{ann}x_3 = (3^4 \cdot 5^4 \cdot 7^3)$，其中 $3^4 \cdot 5^4 \cdot 7^3$ 是上述零化子表中各素元方幂的最小公倍元；

$\text{ann}x_2 = (3^3 \cdot 5^2 \cdot 7)$，其中 $3^3 \cdot 5^2 \cdot 7$ 是上述零化子表中去掉 $3^4, 5^4, 7^3$ 后剩余各素元方幂的最小公倍元；

$\text{ann}x_1 = (3^2)$，其中 3^2 是最后剩余的素元方幂.

从而 $\text{ann}x_1 \supset \text{ann}x_2 \supset \text{ann}x_3$.

反之如果先有第一种直和分解，亦可运用定理 16.7.21(1)将其化成第二种形式.

最后可回答本段开始时提出的模的直和分解是否唯一的问题，有以下定理.

不变性定理 16.7.25 设 M 为主理想整环 D 上的有限生成模，它有如下两个直和分解：

$$M = Dz_1 \oplus Dz_2 \oplus \cdots \oplus Dz_s$$

$$= D\overline{w_1} \oplus D\overline{w_2} \oplus \cdots \oplus D\overline{w_t},$$

其中 $\operatorname{ann} z_1 \supset \operatorname{ann} z_2 \supset \cdots \supset \operatorname{ann} z_s,$

$\operatorname{ann} \overline{w_1} \supset \operatorname{ann} \overline{w_2} \supset \cdots \supset \operatorname{ann} \overline{w_t},$

并且式中没有等于零的项,则

$$s = t.$$

并且 $\operatorname{ann} z_i = \operatorname{ann} \overline{w_i} \quad (1 \leqslant i \leqslant s).$

由不变性定理可见:模的第一种直和分解中的各阶理想及扭模的第二种直和分解中的准素循环子模都是不变的,因此有如下概念和定理.

定义 16.7.26 (1) 在模 M 的第一种直和分解中不变的阶理想序列 $\operatorname{ann} z_1, \operatorname{ann} z_2, \cdots$ 称为 M 的**不变因子理想**(invariant factor ideal).

(2) 在扭模 T 的第二种直和分解中,不变的准素循环子模的阶理想 M_{p_i} 称为 M 的**初等因子理想**(elementary divisor ideal).

定理 16.7.27 (1) 主理想整环 D 上的两个有限生成模 M_1, M_2 同构的充分必要条件是它们有相同的不变因子理想.

(2) 主理想整环 D 上的两个扭模 T_1, T_2 同构的充分必要条件是它们有相同的初等因子理想.

例 16.7.28 (1) 当 $D=\mathbf{Z}$ 时,它的任一理想都有唯一的非负生成元;当 $D=F[\lambda]$,其中 F 是域时,它的每个理想由 0 或一个首 1 多项式(首项系数为 1 的多项式)生成,因而它们的不变因子理想及初等因子理想均可用这些生成元代替,并分别称为各模的不变因子及初等因子.

(2) 设 $D=R[\lambda]$, M 是 D 上循环模的直和,它们的阶理想是由多项式 $(\lambda-1)^3, (\lambda^2+1)^2, (\lambda-1)(\lambda^2+1)^4, (\lambda+2)(\lambda^2+1)^2$ 生成的理想. 则它的初等因子为 $(\lambda^2+1)^2, (\lambda^2+1)^2, (\lambda^2+1)^4, \lambda-1, (\lambda-1)^3, \lambda+2$;它的不变因子为 $d_1=(\lambda^2+1)^2, d_2=(\lambda^2+1)^2(\lambda-1), d_3=(\lambda^2+1)^4(\lambda-1)^3(\lambda+2)$.

16.8 应用

模论主要应用于交换群理论及线性变换理论，本节仅讨论模论在交换群理论中的应用.

将有限生成模理论应用到主理想整环 $D=\mathbf{Z}$ 的场合上去，则 M 是具有有限多个生成元的交换群（特例为有限群），基本定理 16.7.11 断言：任何有限生成的交换群 M 都是循环群的直和：

$$M=\langle z_1\rangle\oplus\langle z_2\rangle\oplus\cdots\oplus\langle z_s\rangle,$$

其中 $\mathrm{ann}z_i=(d_i)$，且 $d_1|d_2|\cdots|d_s$. 当 $d_i\neq 0$ 时，$|d_i|$ 是 z_i 的阶；当 $d_i=0$ 时，z_i 的阶为无限大.

M 的扭子群是由 M 的有限阶元构成的，在上述分解中它与分解 $\langle z_1\rangle+\langle z_2\rangle+\cdots+\langle z_r\rangle$ 一致，其中 $d_1>0,\cdots,d_r>0$，但 $d_{r+1}=0,\cdots,d_s=0$. 由于 $|\langle z_r\rangle|=d_i\ (i\leqslant r)$，所以 $\mathrm{tor}M$ 是阶为 $d_1\cdot d_2\cdot\cdots\cdot d_r$ 的有限群. 定理 16.7.17 则断言，每个有限生成的交换群是一个有限群与一个自由群的直和. 在任何分解中有限部分都像扭子群一样被唯一确定；至于自由群部分可以不是唯一的，但它的秩却是不变的.

运用扭模分解为准素循环模直和的理论可得：任一有限交换群都是若干个阶为素数方幂的循环群的直和，这些素数方幂连同其重复度都是唯一确定的，称它们为这个有限群的不变量，显然两有限群当且仅当它们有相同的不变量时同构.

至此可总结如下.

定理 16.8.1 （1）任何有限生成的交换群都是一个有限群（即它的扭子群）与一个自由群的直和，该自由群的秩是一个不变量.

（2）任何有限交换群都是若干个阶为素数幂的循环群的直和，这些阶连同它们的重复度都是唯一确定的，并且在“两个有限

交换群同构当且仅当它们有相同的不变量集”的意义下，它们构成一个完全不变量集.

例 16.8.2 利用上列结果决定几个有限群的构造如下：

(1) 4 阶交换群只有两种构造，因为 $4=2^2$，其不同的素数幂因子只能有两种组合方式：2，2 及 2^2. 故 4 阶交换群有如下两个：

$M_4^{(1)}=\mathbf{Z}_2\oplus\mathbf{Z}_2$ (Klein 4 元群)

$M_4^{(2)}=\mathbf{Z}_4$ (4 阶循环群)

注： 这里 $\mathbf{Z}_2$、$\mathbf{Z}_4$ 分别是模 2 与模 4 的同余类加群. 这些群的运算根据直和定义应归结到这些同余类群中去. 以下各例均同.

(2) 6 阶交换群只有一种构造，因为 $6=2\times3$，其素数幂因子只有一种组合方式：2，3.

所以 $M_6=\mathbf{Z}_2\oplus\mathbf{Z}_3$.

(3) 24 阶交换群有 3 种构造. 因为 $24=2^3\cdot3=8\cdot3=2\cdot2\cdot2\cdot3=4\cdot2\cdot3$，故

$$M_{24}^{(1)}=\mathbf{Z}_8\oplus\mathbf{Z}_3,$$
$$M_{24}^{(2)}=\mathbf{Z}_2\oplus\mathbf{Z}_2\oplus\mathbf{Z}_2\oplus\mathbf{Z}_3,$$
$$M_{24}^{(3)}=\mathbf{Z}_4\oplus\mathbf{Z}_2\oplus\mathbf{Z}_3.$$

(4) 360 阶交换群的构造有 6 种，这是因为 $360=2^3\cdot3^2\cdot5$，所以

$$M_{360}^{(1)}=\mathbf{Z}_2\oplus\mathbf{Z}_6\oplus\mathbf{Z}_{30},$$
$$M_{360}^{(2)}=\mathbf{Z}_2\oplus\mathbf{Z}_3\oplus\mathbf{Z}_{60},$$
$$M_{360}^{(3)}=\mathbf{Z}_6\oplus\mathbf{Z}_{60},$$
$$M_{360}^{(4)}=\mathbf{Z}_2\oplus\mathbf{Z}_{180},$$
$$M_{360}^{(5)}=\mathbf{Z}_3\oplus\mathbf{Z}_{120},$$
$$M_{360}^{(6)}=\mathbf{Z}_{360}.$$

17 域上的代数

和模的构成相似，域上的代数由作为基集的环 R 与作为其算子集的域 F 构成，就 R 的加法和算子乘法来说它是域 F 上的向量空间，它们间还保持着一定的乘法关系. 由于作为出发点的公理的不同，域上的代数又可分成结合代数和非结合代数两大类，计有外代数、李代数、约当代数、合成代数、交替代数、弹性代数、结合可除代数等等. 本章重点介绍结合代数及结合可除代数并简略介绍李代数及约当代数.

17.1 结合代数的定义及例子

定义 17.1.1 域 F 上的（**结合**）**代数**(associative algebra) A 由一个环 $\langle A;+,\cdot;0,1\rangle$ 及 F 上的一个向量空间 A 构成，其基集 A 及加法与零元"0"在环中及在向量空间中都是一致的，而对于 $a\in F$ 及 $x,y\in A$，则有

$$a(xy)=(ax)y=x(ay).$$

若 A 是 F 上的有限维空间，则称该代数是**有限维的**. 一般情况，各代数仍用其基集 A 表示.

例 17.1.2 (1) 设 F 是域 E 的子域，则 E 是 F 上的一个向量空间，这是因为对于 $a\in F$ 及 $u\in E$，只要按 E 中元素的乘法规定算子乘法 au 即可；E 当然是一个环，又在向量空间与这个环间有相同的加群. 此外还有 $a(uv)=(au)v=u(av)(a\in F,u,v\in E)$，所以 E 是 F 上的(结合)代数. 这时 E 可能是有限维的也可能是无限维的，这完全由 E 是 F 的有限扩域或无限扩域而定.

(2) 设 $F[x]$是域 F 上的一元多项式环，在此环结构上按环的乘法规定算子乘法 $af(x)(a\in F, f(x)\in F[x])$；加法与 0 在两种结构上仍照旧，则它又有了向量空间结构，此外还有

$$a(f(x)g(x))=(af(x))g(x)=f(x)(ag(x)),$$

故 $F[x]$构成 F 上的一个(结合)代数. 这个代数显然是无限维的，因为构成生成元的无限集$\{1,x,x^2,\cdots\}$在 $F[x]$上是线性无关的.

(3) 设 $M_n(F)$是域 F 上的 $n\times n$ 矩阵环，对于 $\forall a\in F$ 及 $\boldsymbol{M}=(m_{ij})$规定 $a\boldsymbol{M}=(am_{ij})$，则 $M_n(F)$又有了 F 上的向量空间结构. 令矩阵 $a\boldsymbol{I}=\mathrm{diag}\{a,a,\cdots,a\}$，则 $a\boldsymbol{I}$[①] 属于环 $M_n(F)$的中心，故 $a\boldsymbol{I}$ 可与每个矩阵交换，因而

$$\begin{aligned}a(\boldsymbol{MN}) &= (a\boldsymbol{I})\boldsymbol{MN} = (a\boldsymbol{M})\boldsymbol{N}\\ &= (\boldsymbol{M}(a\boldsymbol{I}))\boldsymbol{N} = \boldsymbol{M}(a\boldsymbol{N}),\end{aligned}$$

即

$$a(\boldsymbol{MN}) = (a\boldsymbol{M})\boldsymbol{N} = \boldsymbol{M}(a\boldsymbol{N}).$$

故 $M_n(F)$构成 F 上的一个有限维代数，由 n^2 个矩阵单位 e_{ij} 构成的有限集$\{e_{ij}\mid i,j=1,2,\cdots,n\}$就是它的基. 这个代数称为域 F 上的矩阵代数.

(4) 有限群 G 在 F 上的群代数　设 F 是一个域，$G=\{s_1=1, s_2,\cdots,s_n\}$是任一有限群，作

$$F[G]=\left\{\sum_{i=1}^{n}a_is_i \mid a_i\in F\right\},$$

且规定

$$\sum_{i=1}^{n}a_is_i=0\Leftrightarrow a_i=0.$$

按通常方法规定 $F[G]$的元的加法及与 F 的元的算子乘法后，即知 $F[G]$是 F 上的一个向量空间，其基为$\{s_1,s_2,\cdots,s_n\}$.

---

① $a\boldsymbol{I}$ 中的 $\boldsymbol{I}$ 是单位矩阵.

进而规定 $F[G]$的乘积为

$$(\sum_i a_i s_i)(\sum_j b_j s_j) = \sum_{i,j} a_i b_j (s_i s_j),$$

则可证明 $F[G]$是域 F 上的结合代数.

(5) 可在某些环中利用这些环的中心 C 是一个域的事实将它作成 C 上的代数.

由于代数是两栖的，它既有向量空间的结构又有环的结构，因此这两个结构中所有的概念可以平行地移植到代数里去.

定义 17.1.3 (1) 如果代数 A 中的一个子集 B 既是环 A 的子环又是向量空间 A 的子空间，则称 B 为 A 的**子代数**(subalgebra).

(2) 设 S 是代数 A 的一个子集，A 的所有包含 S 的子代数的交集称为**由 S 生成的子代数**(subalgebra generated by # s)，用 $F(S)$表示.

定理 17.1.4 (1) A 的若干个子代数的交集仍是 A 的子代数.

(2) 设 S 是代数 A 的子集，则 $F(S)$是 1 与单项式 $s_{i_1} s_{i_2} \cdots s_{i_r}$ ($s_{i_k} \in S$)的所有 F-线性组合的集，即

$$F(S) = \{a_0 1 + \sum a_{i_1 i_2 \cdots i_r} s_{i_1} \cdots s_{i_r} \mid a_0, a_{i_1 \cdots i_r} \in F\}.$$

定义 17.1.5 设 I 是代数 A 的子集，如果它既是环 A 的理想，又是向量空间 A 的子空间，则称为**代数 A 的理想**(ideal of algebra A).

定义 17.1.6 设 I 是代数 A 的理想，则可得商环 A/I 及差向量空间 A/I，二者结合所构成的代数称为关于理想 I 的商(**或差**)**代数**(quotient/difference algebra).

定义 17.1.7 如果由代数 A 到代数 B(二者在同一域上)的映射既是环同态又是线性映射，则称该映射为**代数同态**(algebraic homomorphism).

类似地可以定义代数的**单态射**、**满态射**、**自同态**及**自同构**.

定理 17.1.8 (1) $\nu: a \mapsto a+I$ 是 A 到 A/I 的一个**标准满态射**(canonical epimorphism).

(2) 设 S 是代数 A 的一个生成元集,η_1 及 η_2 是 A 到 B 的两个代数同态,且 $\forall s \in S$ 都有 $\eta_1(s)=\eta_2(s)$,则 $\eta_1=\eta_2$.

定义 17.1.9 设 η 是 A 到 B 里的代数同态,则集 $K=\eta^{-1}(0)$ 构成 A 的一个理想,该理想称为 η 的**核**,记为 $\ker\eta$.

可以证明:若 I 是包含于 $K=\ker\eta$ 的一个理想,则可诱导出由 A/I 到 B 里面的同态 $\bar{\eta}$ 使得 $\bar{\eta}(a+I)=\eta(a)$,这时在 η 与 $\bar{\eta}$ 间有如下关系:

$$\eta=\bar{\eta}\nu,$$

其中 ν 是 A 到 A/I 上的**标准同态**.

17.2 外代数

外代数是 H. G. Grassmann 于 1844 年提出的一种结合代数,它在几何中特别是在行列式理论中有重要的应用,由它可以推出行列式的主要性质,例如可乘性及 Laplace 展开式定理以及建立可换环上的行列式理论.但由于这些理论早在线性代数中用初等手段实现,本节不再讨论而仅介绍外代数的主要性质及运算公式.

定义 17.2.1 设 V 是 F 上的有限维向量空间,A 是由它生成的代数,若对于 $\forall v \in V$ 都有 $v^2=0$,则称 A 为向量空间 V 的**外代数**(exterior algebra)并用 $E(V)$ 表示.

下面考察外代数 $E(V)$ 的构造:根据前节由 V 生成的代数的定义,$E(V)$ 的每个元必是 1 与单项式 $v_1 v_2 \cdots v_k$ 的 F-线性组合,其中 $k \geqslant 1, v_i \in V$. 若设 $\{u_1, u_2, \cdots, u_n\}$ 是 V 的基,则 $E(V)$ 的每个元是 1 与含 u_i 的单项式的 F-线性组合.

定义 17.2.2 在单项式 $u_{i_1} u_{i_2} \cdots u_{i_r}$ 中,若 $i_1 < i_2 < \cdots < i_r$,则

称元为**标准单项式**(standard monomial).

根据外代数定义中的条件 $v^2=0$,有以下定理.

定理 17.2.3 (1) $u_i{}^2=0$;

(2) $u_iu_j=-u_ju_i$, $1\leqslant i,j\leqslant n$;

(3) $u_{i_1}\ u_{i_2}\ \cdots\ u_{i_r}=(\mathrm{sg}\sigma)\ u_{i_{1'}}\ u_{i_{2'}}\ \cdots\ u_{i_{r'}}$,其中 $\sigma=\begin{pmatrix}1 & 2 & \cdots & r\\ 1' & 2' & \cdots & r'\end{pmatrix}$, $\mathrm{sg}\sigma=1$ 或 -1 根据 σ 是偶排列或奇排列而定.

定理 17.2.4 F 上的有限维向量空间 V 的外代数 $E(V)$ 的每个元都是 1 及标准单项式 $u_{i_1}u_{i_2}\cdots u_{i_r}(i_1<i_2<\cdots<i_r)$ 的一个线性组合,由于这些元可能有相等的及线性相关的,$E(V)$ 的元数必不超过集 $N=\{1,2,\cdots,n\}$ 所能构成的子集 $\{i_1,i_2,\cdots,i_r\}$ 的个数,因而 $\dim E(V)\leqslant|\mathscr{P}(N)|=2^n$.

以下考虑 $E(V)$ 的两个单项式的乘法:设单项式 $u_s=u_{i_1}u_{i_2}\cdots u_{i_r}(i_1<i_2<\cdots<i_r)$,作 $S=\{i_1,i_2,\cdots,i_r\}$,并对 $s,t\in N$ 规定

$$\epsilon_{s,t}=\begin{cases}1, & 若\ s<t;\\ 0, & 若\ s=t;\\ -1, & 若\ s>t.\end{cases}$$

而对 $S,T\subseteq N$ 则规定

$$\epsilon_{S,T}=\begin{cases}\prod\limits_{s\in S,t\in T}\epsilon_{s,t}, & 若\ S\neq\varnothing\ 及\ T\neq\varnothing;\\ 1, & 若\ S\ 或\ T=\varnothing.\end{cases}$$

按此规定可得:

若 $T_1\neq\varnothing$, $T_2\neq\varnothing$,且 $T_1\cap T_2=\varnothing$ 时,则

$$\epsilon_{S,T_1\cup T_2}=\epsilon_{S,T_1}\cdot\epsilon_{S,T_2},$$

$$\epsilon_{T_1\cup T_2,S}=\epsilon_{T_1,S}\cdot\epsilon_{T_2,S}.$$

现规定 $E(V)$ 的两个单项式 u_S 与 u_T 的乘法是

$$u_Su_T=\epsilon_{S,T}u_{S\cup T}.$$

下面再看 $E(V)$ 中任意元的乘法:为了书写简便,将 $E(V)$ 的

元表成 $\sum_{S\in\mathscr{P}(N)} a_S S$ 的形式($a_S\in F$),并规定

$$\left(\sum a_S S\right)\left(\sum b_T T\right)=\sum \epsilon_{S,T} a_S b_T (S\cup T).$$

则可以证明 $E(V)$ 对于这样的规定确可构成结合代数,元 1 及 $u_{i_1}u_{i_2}\cdots u_{i_r}$ 作成它的基,故其维数为 2^n.

关于 V 的外代数有以下定理.

定理 17.2.5 设 L 是空间 V 到代数 A 中的线性映射,满足 $\forall v\in V (Lv)^2=0$ 成立,则 L 可以唯一的方式扩张成为外代数 $E(V)$ 到 A 中的同态 $\eta(L)$.

定理 17.2.6 设 U 是 V 的子空间,则 $E(V)$ 中由 U 生成的子空间同构于 $E(U)$.

定理 17.2.7 若 L 是 V 的线性变换,且 $\eta(L)$ 是 $E(V)$ 的由 L 确定的自同构,则

$$\eta(1)=1,\eta(L_1L_2)=\eta(L_1)\eta(L_2),$$

且在 L 是双射时,$\eta(L)$ 是一个自同构.

定理 17.2.8 设 $E(V)$ 是空间 V 的外代数,则 $E(V)$ 有以下直和分解:

$$E(V)=V\oplus V^2\oplus V^3\oplus\cdots\oplus V^n,$$

其中 V^r 是由各 r 次标准单项式 $u_{i_1}\cdots u_{i_r}$ ($\{u_1,u_2,\cdots,u_n\}$ 是 V 的一组基)生成的空间,且其维数 $\dim V^r=\binom{n}{r}$. $\left(\binom{n}{r}\right.$ 是 n 个 u_i 所能构成的 r 次单项式的个数$\left.\right)$.

17.3 结合代数的正则矩阵表示

在 16.4 节中介绍了加群上的及模上的自同态环,本章将介绍由向量空间的线性变换构成的代数,使得任意结合代数都与它的

一个子代数同构，因而在理论上保证了任意结合代数的可表示性.

定理 17.3.1 设 V 是域 F 上的向量空间，V 的线性变换的集 $\mathrm{End}_F V = \mathrm{Hom}_F(V, V)$ 关于通常意义下的变换的加法与乘法(定理 16.4.1)以及如下规定的数量乘法 $aL = a_V L = L a_V$ 构成结合代数. 其中 $a \in F, L \in \mathrm{End}_F V$(即 L 是 V 的线性变换)，$a_V: x \mapsto ax$(可以证明 a_V 也是 V 的线性变换).

定义 17.3.2 定理 17.3.1 中的代数 $\mathrm{End}_F V$ 称为域 F 上的向量空间 V 的线性变换的(结合)代数.

现仿照 16.5.2 节，利用 F 上的矩阵来研究 $\mathrm{End}_F V$ 中的线性变换及其性质：设 F 上的 V 是一个 n 维向量空间，$\{\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_n\}$ 是它的基，设 $L \in \mathrm{End}_F V$，而关于此基的变换方程及矩阵分别是 $L\boldsymbol{u}_i = \sum_{j=1}^{n} l_{ij}\boldsymbol{u}_j (i = 1, 2, \cdots, n)$ 及 $\boldsymbol{\Lambda} = (l_{ij})$；今取另一基 $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n\}$，设 $\boldsymbol{v}_i = \sum_{j=1}^{n} c_{ij}\boldsymbol{u}_j (i = 1, 2, \cdots, n)$ 而且 $\boldsymbol{\Gamma} = (c_{ij})$ 是可逆的，则相似矩阵 $\boldsymbol{\Gamma\Lambda\Gamma}^{-1}$ 是 L 关于基 $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n\}$ 的矩阵.

定义 17.3.3 设线性变换 L 关于基 $\{\boldsymbol{u}_i\}$ 的矩阵为 $\boldsymbol{\Lambda} = (l_{ij})$，则 $f(\lambda) = \det(\lambda \boldsymbol{I} - \boldsymbol{\Lambda}) = \lambda^n - \left(\sum l_{ij}\right)\lambda^{n-1} + \cdots + (-1)^n \det\boldsymbol{\Lambda}$ 称为矩阵 $\boldsymbol{\Lambda}$ 的**特征多项式**(characteristic polynomial)；元 $\sum l_{ij}$ 称为 $\boldsymbol{\Lambda}$ 的**迹**(trace)，用 $\mathrm{tr}\boldsymbol{\Lambda}$ 表示；行列式 $\det\boldsymbol{\Lambda}$ 称为 $\boldsymbol{\Lambda}$ 的**范数**(norm).

定理 17.3.4 (1) 若矩阵 $\boldsymbol{M}$ 与 $\boldsymbol{\Lambda}$ 相似(即 $\boldsymbol{M} = \boldsymbol{\Gamma\Lambda\Gamma}^{-1}$)，则它们有相同的特征多项式，因而亦有相同的迹和范数.

(2) $\mathrm{tr}(\boldsymbol{\Lambda}_1 + \boldsymbol{\Lambda}_2) = \mathrm{tr}\boldsymbol{\Lambda}_1 + \mathrm{tr}\boldsymbol{\Lambda}_2$,

$\mathrm{tr}a\boldsymbol{\Lambda} = a\,\mathrm{tr}\boldsymbol{\Lambda}$.

(3) $\det\boldsymbol{\Lambda}_1\boldsymbol{\Lambda}_2 = \det\boldsymbol{\Lambda}_1 \cdot \det\boldsymbol{\Lambda}_2$,

$\det a\boldsymbol{\Lambda} = a^n \det\boldsymbol{\Lambda}$.

定理 17.3.5 从 $\mathrm{End}_F V$ 到(在同一基下)矩阵代数 $M_n(F)$ 中

的映射 $\sigma: L\to \boldsymbol{\Lambda}$ 是一个环反同构，即 σ 是双射而且若 $\sigma: L_1\mapsto \boldsymbol{\Lambda}_1$，$L_2\mapsto \boldsymbol{\Lambda}_2$，则

$$\sigma: L_1+L_2\mapsto \boldsymbol{\Lambda}_2+\boldsymbol{\Lambda}_1, L_1\cdot L_2\mapsto \boldsymbol{\Lambda}_2\cdot \boldsymbol{\Lambda}_1.$$

定理 17.3.6 任一(结合)代数 A 均同构于 F 上的向量空间 A 的线性变换代数 $\mathrm{End}_F A$ 的一个子代数.

以下介绍代数的表示问题.

定义 17.3.7 F 上的代数 A 到 F 上向量空间 V 的线性变换代数 $\mathrm{End}_F V$ 中的一个同态称为 A 的一个**表示**(representation).

定义 17.3.8 对于代数 A 的每个元 u 使 $\mathrm{End}_F A$ 的 $u_L: x\mapsto ux(x\in A)$ 与之对应，则 $\sigma: u\mapsto u_L$ 称为 A 的一个**正则表示**(regular representation).

定义 17.3.9 在代数 A 用线性变换表示的前提下，若用与 $\mathrm{End}_F V$ 反同构的 $M_n(F)$ 的矩阵代替，则此同态称为 A 的**矩阵表示**(matrix representation).

定义 17.3.10 有限维代数 A 的与正则表示联系的矩阵表示称为 A 的**正则矩阵表示**(regular matrix representation).

例 17.3.11 (1) 可以证明四元数除环 H(见 15.2.2 节)构成数域 $\mathbf{R}$ 上的一个结合代数，称为 **Hamilton 的四元代数**，它在 $\mathbf{R}$ 上的维数为 4，$\{1,\mathrm{i},\mathrm{j},\mathrm{k}\}$ 构成它的基，其乘法表如例 15.2.6 所示. 任取 $u=a_0+a_1\mathrm{i}+a_2\mathrm{j}+a_3\mathrm{k}\in H$，则

$$\begin{aligned}
u\cdot 1&= a_0+a_1\mathrm{i}+a_2\mathrm{j}+a_3\mathrm{k},\\
u\cdot \mathrm{i}&=-a_1+a_0\mathrm{i}+a_3\mathrm{j}-a_2\mathrm{k},\\
u\cdot \mathrm{j}&=-a_2-a_3\mathrm{i}+a_0\mathrm{j}+a_1\mathrm{k},\\
u\cdot \mathrm{k}&=-a_3+a_2\mathrm{i}-a_1\mathrm{j}+a_0\mathrm{k}.
\end{aligned}$$

对应的矩阵表示是

$$\Lambda(u)=\begin{bmatrix} a_0 & -a_1 & -a_2 & -a_3 \\ a_1 & a_0 & -a_3 & a_2 \\ a_2 & a_3 & a_0 & -a_1 \\ a_3 & -a_2 & a_1 & a_0 \end{bmatrix},$$

(注意这里已将系数矩阵转置!)

经过计算可以求得迹及范数为

$$T(u)=4a_0,$$

$$N(u)=(a_0{}^2+a_1{}^2+a_2{}^2+a_3{}^2)^2.$$

(2) 设 $A=F[u]$,其中 u 是 F 上的代数,且其最小多项式为 $p(x)=x^n-a_{n-1}x^{n-1}-\cdots-a_0$,则 $A\cong F[x]/p(x)$(定理 15.11.8),现取基$\{1,u,\cdots,u^{n-1}\}$,则因

$$u\cdot 1=u,$$

$$u\cdot u=u^2,$$

$$\vdots$$

$$u\cdot u^{n-2}=u^{n-1},$$

$$u\cdot u^{n-1}=u^n=a_0+a_1u+\cdots+a_{n-1}u^{n-1}.$$

故其正则矩阵表示是

$$\rho(u)=\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-1} \end{bmatrix}.$$

作为特例,现取 $f(x)=x^n-1$,则容易求得最小多项式为

$$y=y_0+y_1u+y_2u^2+\cdots+y_{n-1}u^{n-1},$$

相应地

$$\boldsymbol{\rho}(y)=\begin{bmatrix} y_0 & y_{n-1} & y_{n-2} & \cdots & y_1 \\ y_1 & y_0 & y_{n-1} & \cdots & y_2 \\ y_2 & y_1 & y_0 & \cdots & y_3 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ y_{n-1} & y_{n-2} & y_{n-3} & \cdots & y_0 \end{bmatrix}.$$

(3) 设 A 是基为 $\{\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_n\}$ 的代数，而且 $\boldsymbol{e}_i^2=\boldsymbol{e}_i$，$\boldsymbol{e}_i\boldsymbol{e}_j=0(i\neq j)$. 现设 $\boldsymbol{x}=\sum_{i=1}^{n}\boldsymbol{x}_i\boldsymbol{e}_i$，则由此基确定的

$$\begin{aligned}\boldsymbol{\rho}(\boldsymbol{x})&=\operatorname{diag}\{x_1,x_2,\cdots,x_n\}\\&=\begin{bmatrix} x_1 & & & \\ & x_2 & & \\ & & \ddots & \\ & & & x_n \end{bmatrix}.\end{aligned}$$

17.4 非结合代数、李代数及约当代数

17.4.1 非结合代数

本节介绍的非结合代数是指对乘法结合律不作要求的代数，因此它可以是结合的或是不满足乘法结合律的代数，本节介绍的李(Lie)代数和约当(Jordan)代数都是不满足乘法结合律的. 此外还有弹性代数(elastic algebra)、合成代数(composition algebra)、交错代数(alternative algebra)等.

定义 17.4.1 若域 F 上的向量空间 A 有双线性的二元运算 $(x,y)\mapsto xy$ 使

$$\begin{aligned}(x_1+x_2)y&=x_1y+x_2y,\\x(y_1+y_2)&=xy_1+xy_2,\\a(xy)&=(ax)y=x(ay).\end{aligned}$$

则称 A 为域 F 上的**非结合代数**(non-associative algebra).

将此定义与定义 17.1.1 对比，可以看出，那里要求 A 是一个环，根据环的定义它具有乘法而且满足结合律，这个要求在本定义中是没有的.

17.1 节中各例的结合代数当然都是非结合代数，它们各自的乘法就是这里的双线性的二元运算.

以下将分别介绍不满足乘法结合律的非结合代数.

17.4.2 李代数

定义 17.4.2 设域 F 上的非结合代数 L 内的二元运算 $[xy]$（或 $[x,y]$）满足下列两个条件：

(1) $[xx]=0$,

(2) $[[xy]z]+[[yz]x]+[[zx]y]=0$,

则称 L 为域 F 上的**李代数**(Lie algebra).

注 关于定义的两点说明：

1) 条件(1)在特征 $\neq 2$ 的域 F 上是与以下条件等价的：

$$\circledast \quad [xy]=-[yx] \qquad \text{(反交换性)}.$$

这是因为：由 $\circledast \Rightarrow$ (1) 是显然的，只要令 $y=x$ 得 $2[xx]=0$ 及由 F 的特征 $\neq 2$ 即可得到；反之，若在(1)中将 $x+y$ 代 x 并按分配律展开即得

$$\begin{aligned}0 &=[(x+y)(x+y)]=[xx]+[xy]+[yx]+[yy] \\ &=[xy]+[yx],\end{aligned}$$

从而 $[xy]=-[yx]$.

2) 条件(2)称为雅可比(Jacobi)恒等式，它的第 2,3 项是由第 1 项经过 x,y,z 的循环置换得到的.

例 17.4.3 (1) 设 A 是域 F 上的任一结合代数，在向量空间 A 内定义交换子乘积 $[xy]=xy-yx$ 就能将它构成李代数 A^{-}，这是因为 $[xx]=xx-xx=0$，而且

$$[[xy]z]=(xy-yx)z-z(xy-yx)$$

$$= xyz - yxz - zxy + zyx,$$

$$[[yz]x] = (yz - zy)x - x(yz - zy)$$

$$= yzx - zyx - xyz + xzy,$$

$$[[zx]y] = (zx - xz)y - y(zx - xz)$$

$$= zxy - xzy - yzx + yxz.$$

把三式相加即得雅可比恒等式.

特别地,令 $M_n(\mathbf{R})$代表实数域 $\mathbf{R}$ 上的 $n\times n$ 矩阵构成的结合代数,若在其中引入交换子乘积$[\boldsymbol{XY}]=\boldsymbol{XY}-\boldsymbol{YX}$,则可得李代数 $M_n(\mathbf{R})^-$.

又如 A 是域 F 上的任一非结合代数,A 作为向量空间时的全体线性变换的代数 $\mathrm{End}_F A$ 亦可类似地构成一个李代数 $\mathrm{End}_F A^-$,这只要在其中引入交换子乘积

$$[L_1L_2] = L_1L_2 - L_2L_1.$$

此外,还可利用李代数的子代数构成新的李代数.下面就上例中的两个具体李代数说明这种构作法.对于子李代数的意义按通常的子结构的意义理解,即李代数 L 关于它的所有运算(其中包括交换子乘积)均为封闭的非空子集所构成的子代数结构.

(2) 结合代数 A 的一个反自同构 $j:x\mapsto\bar{x}$,如果满足 $j^2=1$,则称 j 为**对合**(involution).例如 $A=M_n(F)$的转置映射 $t:\boldsymbol{X}\mapsto {}^t\boldsymbol{X}(\boldsymbol{X}\in M_n(F))$就是一个对合;又如 $M_n(F)$的元 $\boldsymbol{S}$ 到 $-\boldsymbol{S}$ 的映射 $j:\boldsymbol{S}\mapsto-\boldsymbol{S}$ 也是,满足这个条件的元称为 ***j*-斜元**(j-skew element),即 $\bar{\boldsymbol{S}}=-\boldsymbol{S}$ 的元.今令 $\mathrm{SK}(A,j)$表示 A 的 j-斜元 $\boldsymbol{S}$ 所成的集,则当 $\boldsymbol{S}_1,\boldsymbol{S}_2\in\mathrm{SK}(A,j)$及 $a_1,a_2\in F$ 时 $a_1\boldsymbol{S}_1+a_2\boldsymbol{S}_2\in\mathrm{SK}(A,j)$及$[\boldsymbol{S}_1\boldsymbol{S}_2]\in\mathrm{SK}(A,j)$,这是因为

$$\overline{a_1\boldsymbol{S}_1+a_2\boldsymbol{S}_2}=a_1\overline{\boldsymbol{S}_1}+a_2\overline{\boldsymbol{S}_2}=a_1(-\boldsymbol{S}_1)+a_2(-\boldsymbol{S}_2)$$

$$=-(a_1\boldsymbol{S}_1+a_2\boldsymbol{S}_2),$$

$$\overline{[\boldsymbol{S}_1\boldsymbol{S}_2]}=\overline{\boldsymbol{S}_1\boldsymbol{S}_2-\boldsymbol{S}_2\boldsymbol{S}_1}=\bar{\boldsymbol{S}}_2\bar{\boldsymbol{S}}_1-\overline{\boldsymbol{S}_1}\ \overline{\boldsymbol{S}_2}$$

$$=(-\boldsymbol{S}_2)(-\boldsymbol{S}_1)-(-\boldsymbol{S}_1)(-\boldsymbol{S}_2)=-(\boldsymbol{S}_1\boldsymbol{S}_2-\boldsymbol{S}_2\boldsymbol{S}_1)$$
$$=-[\boldsymbol{S}_1\boldsymbol{S}_2].$$

故 $\mathrm{SK}(A,j)$ 是 A^- 的一个子李代数，因而也是李代数.

(3) 在李代数 $\mathrm{End}_F A^-$ 中定义 A 的微分 D 为 A 到 A 的满足下式的线性映射：

$$D(xy)=(Dx)y+x(Dy) \qquad (x,y\in A).$$

取 A 的微分所成的集 $\mathrm{Der}A$，则可证：

若 $D_1,D_2\in\mathrm{Der}A, a\in F$，则 $D_1+D_2\in\mathrm{Der}A$ 及 $aD\in\mathrm{Der}A$.

又因 $D_1D_2(xy)=D_1((D_2x)y+x(D_2y))$

$$=(D_1Dx)y+(D_1x)(D_2y)+(D_2x)(D_1y)+x(D_1D_2y)$$

及 $(D_1x)(D_2y)+(D_2x)(D_1y)$ 关于 D_1,D_2 的对称性及反交换性知此和为零，因而 $D_1D_2\in\mathrm{Der}A$. 故 $\mathrm{Der}A$ 作成 $\mathrm{End}_F A^-$ 的一个子代数，称为非结合代数 A 的**微分代数**(derivation algebra).

定理 17.4.4 李代数的交换子乘积不满足结合律. 该定理可用反证法证明：若 $[[xy]z]=[x[yz]]$，则必有 $[y[xz]]=0$. 今取 $A=M_2(F)$，从中取出 $\boldsymbol{X}=\boldsymbol{Y}=\boldsymbol{E}_{12}, \boldsymbol{Z}=\boldsymbol{E}_{21}$，则 $[\boldsymbol{Y}[\boldsymbol{XZ}]]=-2\boldsymbol{E}_{12}\neq\boldsymbol{0}$. 这就证明了它不满足结合律.

17.4.3 约当代数

定义 17.4.5 一个特征 $\neq 2$ 的域 F 上的非结合代数，如果它的乘法 $x\cdot y$(通称为约当乘积或反交换子)满足以下法则：

(1) $x\cdot y=y\cdot x$,

(2) $(x^{\cdot 2}\cdot y)\cdot x=x^{\cdot 2}\cdot(y\cdot x)$，其中 $x^{\cdot 2}=x\cdot x$，则称该代数为域 F 上的**约当代数**(Jordan algebra).

注意：(2)中各方幂的指数前带有“$\cdot$”号，表示若干个相同的元作约当乘积的结果；该等式称为约当恒等式，它表示一种特殊的

"结合律".

例 17.4.6 (1) 在任一特征不为 2 的域 F 上的结合代数 A 中引入称为反交换子的约当乘积：

$$x \cdot y = \frac{1}{2}(xy + yx),$$

则确定约当代数 A^+：因为这个乘积显然是可交换的，故有(1)；至于它适合法则(2)可以通过直接验证得到：

$$\begin{aligned}(x^{\cdot 2} \cdot y) \cdot x &= \{[(x \cdot x) \cdot y] \cdot x\} = \left(\frac{xx + xx}{2} \cdot y\right) \cdot x \\ &= (x^2 \cdot y) \cdot x = \frac{x^2 y + yx^2}{2} \cdot x \\ &= \frac{1}{2}\left(\frac{x^2 y + yx^2}{2} x + x \frac{x^2 y + yx^2}{2}\right) \\ &= \frac{1}{4}(x^2 yx + yx^3 + x^3 y + xyx^2).\end{aligned}$$

同法可证

$$x^{\cdot 2} \cdot (y \cdot x) = \frac{1}{4}(x^2 yx + x^3 y + yx^3 + xyx^2).$$

故$(x^{\cdot 2} \cdot y) \cdot x = x^{\cdot 2} \cdot (y \cdot x)$，即法则(2)成立.

(2) 还可利用上述约当代数 A^+ 的子代数构成约当代数. 例如设 A 有一对称 j(例 17.4.3(2))时，则由 A 的 j-对称元 s(A 的满足 $\bar{s} = j(s) = s$ 的元)组成的集 $Sym(A, j)$ 构成一个子约当代数. 这是因为如果 $h_1, h_2 \in Sym(A, j)$ 且 $a_1, a_2 \in F$，则 $\bar{h} = \overline{(a_1 h_1 + a_2 h_2)} = a_1 \overline{h_1} + a_2 \overline{h_2} = a_1 h_1 + a_2 h_2 = h$，所以 $Sym(A, j)$ 构成子空间；又因如果$h_1, h_2 \in Sym(A, j)$，则 $\bar{h} = \overline{h_1 \cdot h_2} = \overline{\frac{1}{2}(h_1 h_2 + h_2 h_1)} = \frac{1}{2}(\overline{h_2}\ \overline{h_1} + \overline{h_1}\ \overline{h_2}) = \frac{1}{2}(h_2 h_1 + h_1 h_2) = h_1 \cdot h_2 = h$，所以 $h_1 \cdot h_2 \in Sym(A, j)$.

所以 $Sym(A,j)$ 构成 A^+ 的子空间.

下面介绍约当代数的一些运算法则:

定理 17.4.7 约当代数的乘法不满足结合律.

本定理可利用的 Jordan 乘积 $x \cdot y = \frac{1}{2}(xy+yx)$ 直接计算证明之,经计算得

$$(x \cdot y) \cdot z = \frac{1}{4}(xyz + yxz + zxy + zyx),$$

$$x \cdot (y \cdot z) = \frac{1}{4}(xyz + xzy + yzx + zyx),$$

所以 $(x \cdot y) \cdot z - x \cdot (y \cdot z) = \frac{1}{4}(yxz + zxy - xzy - yzx)$

$$= \frac{1}{4}[y[xz]].$$

后者是李代数的交换子乘积,它不满足结合律(定理 17.4.4),因而 Jordan 乘积也是不满足结合律的.

利用交换子乘积[]与约当乘积“·”间的以上关系及雅可比恒等式(定义 17.4.2(2))可得如下公式.

公式 17.4.8 $(x \cdot y) \cdot z - x \cdot (y \cdot z) + (y \cdot z) \cdot x - y \cdot (z \cdot x) + (z \cdot x) \cdot y - z \cdot (x \cdot y) = 0$

利用归纳法可得如下公式.

公式 17.4.9 **幂结合律** 设 $k, l \in \mathbf{N}$,则

$x^{\cdot k} \cdot x^{\cdot l} = x^{\cdot (k+l)}$.

定义 17.4.10 设 x, y, z 是非结合代数 A 的任意三个元,则 $[x,y,z] = (xy)z - x(yz)$ 称为 x, y, z 的**结合子**(associator).

利用结合子可将 Jordan 恒等式表成下式:

$$[x^2, y, x] = 0.$$

可以证明,结合子是一个三重线性函数,即它的三个变项都是

线性的,例如$[x_1+x_2,y,z]=[x_1,y,z]+[x_2,y,z]$,$[x,y_1+y_2,z]=[x,y_1,z]+[x,y_2,z]$等等以及 $a[x,y,z]=[ax,y,z]=[x,ay,z]=[x,y,az]$. 利用这个性质可得以下公式.

公式 17.4.11 $[x_1\cdot x_2,y,x_3]+[x_2\cdot x_3,y,x_1]+[x_3\cdot x_1,y,x_2]=0$.

定义 17.4.12 设 A 是任一非结合代数,其上线性映射 x_L: $y\mapsto xy$ 及x_R:$y\mapsto yx$($\forall y\in A$)分别称为**用 x 左乘或右乘**.

利用左、右乘符号可将约当代数的一些公式简化如下.

公式 17.4.13 (1) $x_L=x_R$. (交换律)

(2) $(x^{\cdot 2})_L=x_L(x^{\cdot 2})_L$或$[(x^{\cdot 2})_L,x_L]=0$.(约当恒等式)(因约当乘积适合交换律,$x_L=x_R$及$(x^{\cdot 2})_L=(x^{\cdot 2})_R$).

(3) 公式 17.4.11 可简化成

$[(x_1\cdot x_2)_L,(x_3)_L]+[(x_2\cdot x_3)_L,(x_1)_L]+[(x_3\cdot x_1)_L,(x_2)_L]=0$.

17.5 有限维结合可除代数

环及代数结构理论的一个主要结果是将某些普通环类的研究化归到除环上去,在有限维代数的情形则将它化归到可除代数,为此就基础域是代数闭域(定义 15.13.1)、实数域 **R** 及有限域三种情况讨论,现简述其主要结论如下.

定义 17.5.1 设 A 是域 F 上的有限维结合代数,若它的每个非零元都在 A 内有逆元,则称 A 为**有限维结合可除代数**(finite dimensional associative division algebra).

定理 17.5.2 若 F 是代数闭域,则仅有 F 自身是 F 上的有限维结合可除代数.

定理 17.5.3 **Frobenius 定理** 实数域 **R** 上的有限维结合可

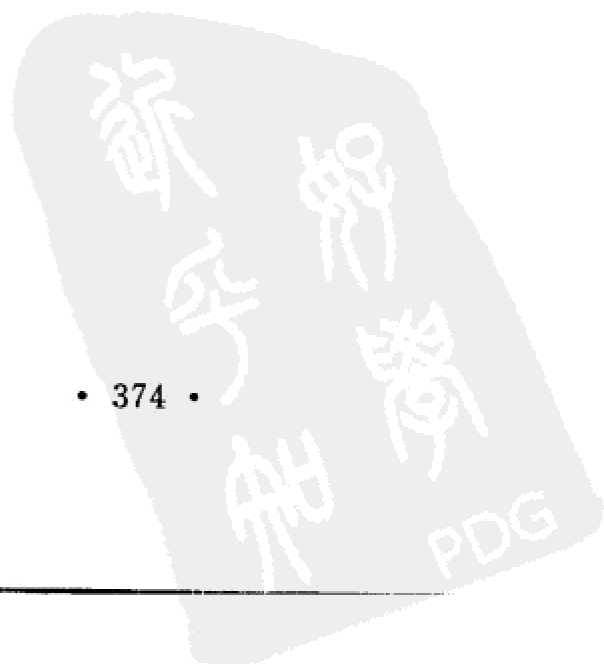
除代数仅有以下三种：

(1) 实数域 **R**；

(2) 复数域 **C**；

(3) 四元数除环 H.

定理 17.5.4 Wedderburn 定理 有限除环都是交换环，因而都是域.



18 格与 Boole 代数

本章从偏序集出发介绍格及布尔代数. 后者自 19 世纪中期公开发表之时起就已逐步成为研究人类思维规律的重要工具，20 世纪 30 年代以后广泛应用于电子线路及芯片设计，目前布尔代数已成为计算机科学的重要基础理论之一.

18.1 偏序集与格

定义 18.1.1 设 P 是集，P 上的二元关系"$\leqslant$"若能满足以下三个条件，则称"$\leqslant$"是 P 上的**偏序关系**(partial order relation)(或**部分序关系**)：

(1) 自反性：$\forall a\in P, a\leqslant a$；

(2) 反对称性 $\forall a,b\in P$，若 $a\leqslant b$ 且 $b\leqslant a$，则 $a=b$；

(3) 传递性：$\forall a,b,c\in P$，若 $a\leqslant b$ 且 $b\leqslant c$，则 $a\leqslant b$.

具有偏序关系"$\leqslant$"的集 P 称为**偏序集**(partial order set)，记为 $\langle P;\leqslant\rangle$. 特别地，设 S 是偏序集，若对于 $\forall a,b\in S$ 都有 $a\leqslant b$ 或 $b\leqslant a$，则称 S 是**全序集**(total order set)或**链**(chain).

说明：(1) 若 $a\leqslant b$ 且 $a\neq b$，则简记为 $a<b$；

(2) $a\leqslant b$ 可改写为 $b\geqslant a$，同理 $a<b$ 亦可改写为 $b>a$.

例 18.1.2 (1) 在 $\mathbf{R}$ 中，"$\leqslant$"表示实数间的小于或等于关系，则"$\leqslant$"为偏序关系；$\langle \mathbf{R};\leqslant\rangle$ 是偏序集，同时，它也是全序集.

(2) 设 A 是任意集，$\mathscr{P}(A)$ 是它的幂集，即 A 的全部子集所构成的集，"$\leqslant$"表示 $\mathscr{P}(A)$ 的元间的包含关系"$\subseteq$"，则 $\langle \mathscr{P}(A);\subseteq\rangle$ 是偏序集.

(3) 在 $\mathbf{N}^+$ 中，"$\leqslant$"表示两个正整数间的整除关系，即 $a,b\in\mathbf{N}^+$，$a\leqslant b\Leftrightarrow a\mid b$，则"$\leqslant$"为偏序关系，$\langle\mathbf{N}^+;\leqslant\rangle$是偏序集.

对于有限集 P，偏序关系通常用 Hasse 图表示，这种图形用线段的端点表示 P 的元，而将连接上下两个端点的线段表示关系"$\leqslant$"，若端点 a 在 b 的下方则表示 $a\leqslant b$.

(4) 设 $A=\{a,b\}$，A 的幂集 $\mathscr{P}(A)=\{\varnothing,\{a\},\{b\},\{a,b\}\}$，则偏序集$\langle\mathscr{P}(A);\subseteq\rangle$的图形如图 18.1.

(5) 设 $P=\{1,2,3,4,6,8,9,12,18,24\}$，偏序关系"$\leqslant$"为整除关系，则$\langle P;\leqslant\rangle$是一个偏序集，如图 18.2.

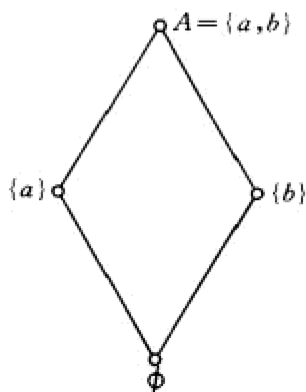


图 18.1

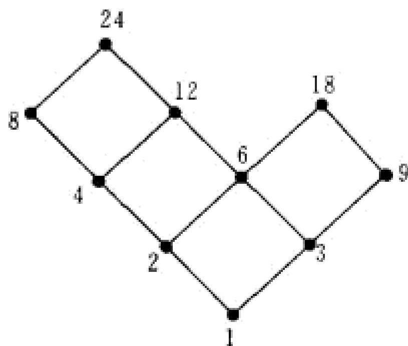


图 18.2

定义 18.1.3 设$\langle P;\leqslant\rangle$是偏序集，如果 P 的元 m 对于 $\forall x\in P$ 都有 $m\leqslant x$，则称 m 为 P 的**最小元**(least element)；反之，如果 P 的元 n 对于 $\forall x\in P$ 都有 $x\leqslant n$，则称 n 为 P 的**最大元**(greatest element).

例 18.1.4 例 18.1.2(4) $\langle\mathscr{P}(A);\subseteq\rangle$中的 A 是最大元，而$\varnothing$是最小元；例 18.1.2(5) 中$\langle P;\leqslant\rangle$的最小元为 1，它没有最大元.

定义 18.1.5 设$\langle P;\leqslant\rangle$是偏序集，$T$ 是 P 的子集，如果对于 $\forall x\in T$ 都有 $x\leqslant u$($u\leqslant x$)，则 P 的元 u 称为 T 的**上(下)界**(upper (lower) bound).

定义 18.1.6 设$\langle P;\leqslant\rangle$是偏序集，$T$是$P$的子集，如果对于$T$的任意上界$x$都有$u\leqslant x$，则$T$的上界$u$称为**最小上界**(least upper bound)，记为$u=\sup T$；另一方面，如果对于T的任意下界x均有$x\leqslant v$，则T的下界v称为**最大下界**(greatest lower bound)，记为$v=\inf T$.

注意：偏序集不一定有上界和下界，而且子集T即使有上下界，这些界也未必在T之中. 此外，子集T的最小上界或最大下界如果存在的话，那么它们必是唯一的.

例 18.1.7 (1) 设集$P=\{2,3,6,12,24,36\}$，偏序关系"$\leqslant$"为整数的整除关系，则偏序集$\langle P;\leqslant\rangle$见图 18.3.

若取子集$T_1=\{2,3,6\}$，则$\sup T_1=6$，但$\inf T_1$不存在；若取$T_2=\{2,3\}$，则$\sup T_2=6(\notin T_2)$，但$\inf T_2$不存在；若取$T_3=\{6,12\}$，则$\sup T_3=12$，$\inf T_3=6$.

(2) 设集$A=\{a,b,c\}$，$\mathscr{P}(A)$是其幂集，偏序集$\langle\mathscr{P}(A);\subseteq\rangle$如图 18.4. 易见其最大元为$A$，最小元为$\varnothing$，若取$\mathscr{P}(A)$的子集$T_1=\{\{b,c\},\{b\},\{c\}\}$，则$A$与$\{b,c\}$是$T_1$的上界而$\sup T_1=\{b,c\}$；$\varnothing$是$T_1$的下界，也是它的 inf. 若取$T_2=\{\{a\},\{b\}\}$，则$\sup T_2=\{a,b\}$，而$\inf T_2=\varnothing$.

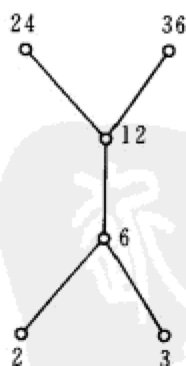


图 18.3

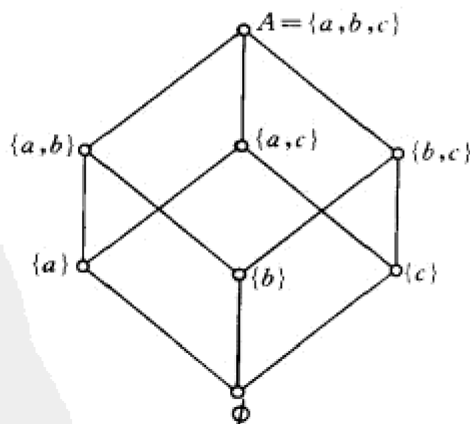


图 18.4

定义 18.1.8 设$\langle L;\leqslant\rangle$是偏序集，如果 L 中任意两个元均有最小上界与最大下界，则称$\langle L;\leqslant\rangle$是**格**(lattice).

例 18.1.9 (1) 取 $L=\mathbf{R}$，偏序关系为实数的小于等于关系"$\leqslant$"，则$\langle \mathbf{R};\leqslant\rangle$是格，因为 $\mathbf{R}$ 的任二实数的 $\sup\{x,y\}=\max\{x,y\}$，$\inf\{x,y\}=\min\{x,y\}$.

(2) 设 A 是任意集，其幂集 $\mathscr{P}(A)$关于集的包含关系"$\subseteq$"构成格$\langle\mathscr{P}(A);\subseteq\rangle$，因为它是偏序集，而且对于 $\forall S,T\in\mathscr{P}(A)$，$\sup\{S,T\}=S\cup T$，$\inf\{S,T\}=S\cap T$.

(3) 整数 110 的正整数因子集 $L=\{1,2,5,10,11,22,55,110\}$，偏序关系"$\leqslant$"为整除关系，则它是偏序集$\langle L;\leqslant\rangle$. 由图 18.5 可见，$L$ 中的任意两个数都有 sup 及 inf，故$\langle L;\leqslant\rangle$是格.

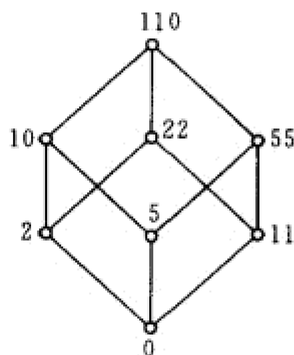


图 18.5

(4) 任一全序集都是格.

定义 18.1.10 格$\langle L;\leqslant\rangle$中的二元运算：

$\vee:(a,b)\mapsto\sup\{a,b\}\ (a,b\in L)$.

$\wedge:(a,b)\mapsto\inf\{a,b\}\ (a,b\in L)$.

分别称为元 a,b 的**并**(union)及**交**(meet)，记作：

$a\vee b=\sup\{a,b\}$，

$a\wedge b=\inf\{a,b\}$.

定理 18.1.11 设$\langle L;\leqslant\rangle$是格，在其上规定的并与交有以下性质：设 $a,b\in L$，则：

(1)[①] $a,b\leqslant a\vee b$，$a\wedge b\leqslant a,b$；

(2) $a\leqslant b\Leftrightarrow a\vee b=b\Leftrightarrow a\wedge b=a$.

定理 18.1.12 (1) 设$\langle L;\leqslant\rangle$是格，在其上规定二元运算$\vee$、

① $a,b\leqslant a\vee b$ 的意思是 $a\leqslant a\vee b$ 而且 $b\leqslant a\vee b$.
$a\wedge b\leqslant a,b$ 的意思是 $a\wedge b\leqslant a$ 而且 $a\wedge b\leqslant b$.

$\wedge$后，必有以下规律：

1) 幂等律

$$a \vee a = a, a \wedge a = a.$$

2) 交换律

$$a \vee b = b \vee a, a \wedge b = b \wedge a.$$

3) 结合律

$$(a \vee b) \vee c = a \vee (b \vee c),$$
$$(a \wedge b) \wedge c = a \wedge (b \wedge c).$$

4) 吸收律

$$a \vee (a \wedge b) = a, a \wedge (a \vee b) = a.$$

(2) 在集 L 上定义两个二元运算 $\vee$ 与 $\wedge$ 使满足(1)中的四条规律，则 $\langle L; \vee, \wedge \rangle$ 构成一个格.

由此可得格的另一定义.

定义 18.1.13 设集 L 具有两个满足定理 18.1.12 的规律 1)～4)的二元运算 $\vee$、$\wedge$，则称 $\langle L; \vee, \wedge \rangle$ 为**格**.

读者不难验证例 18.1.9 中各例的 L 是格，其中与(1)相应的 $\vee$ 是"求大数"，$\wedge$ 是"求小数"；与(2)相应的 $\vee$ 是求二集的并 $\cup$，而 $\wedge$ 则是求二集的交 $\cap$；与(3)相应的 $\vee$ 与 $\wedge$ 分别是求二正整数的最小公倍数与最大公约数；(4)中的 $\vee$ 与 $\wedge$ 是求二元的 sup 与 inf.

由于这两种定义是等价的，今后在讨论格时可以同时使用其上的运算及偏序关系，只要记住它们之间的关系.

定理 18.1.14 设 $\langle L; \leqslant \rangle$ 是格，$\forall a, b, c, d \in L$，则以下各式成立：

(1) $b \leqslant c \Rightarrow a \vee b \leqslant a \vee c, a \wedge b \leqslant a \wedge c$;

(2) $a \leqslant b, c \leqslant d \Rightarrow a \vee c \leqslant b \vee d, a \wedge c \leqslant b \wedge d$.

定理 18.1.15 **对偶原理**(principle of duality) 设 S 是有关偏序集的真命题，则将其中的所有"$\leqslant$"与"$\geqslant$"对换(或将其中的 $\vee$ 与 $\wedge$ 对换)后所得的对偶命题也是真命题.(例如定理 18.1.12 中

的两个幂等律就是互为对偶的等式，它们都是真命题；此外，成对出现的交换律、结合律及吸收律也说明了此种现象.）

18.2 子格与格同态

定义 18.2.1 设$\langle L;\vee,\wedge\rangle$是格，$T$是$L$的非空子集，如果$T$关于$\vee$，$\wedge$封闭（即$\forall a,b\in T\Rightarrow a\vee b$及$a\wedge b\in T$），则称$\langle T;\vee,\wedge\rangle$是$\langle L;\vee,\wedge\rangle$的**子格**(sub lattice).

例 18.2.2 （1）设$\mathbf{N}^+$是正整数集，规定$a\vee b=[a,b]$（即a,b的最小公倍数(lcm)），$a\wedge b=(a,b)$（即a,b的最大公约数(gcd)），则由定义 18.1.13 知$\langle\mathbf{N}^+;\vee,\wedge\rangle$是格.现取正偶数集$E$为其子集，则因二偶数的 lcm 及 gcd 仍是偶数，因而E关于$\vee$与$\wedge$是封闭的，故$\langle E;\vee,\wedge\rangle$是格$\langle\mathbf{N}^+;\vee,\wedge\rangle$的子格.

（2）设a,b是格L的固定元，且$a\leqslant b$，则$T_1=\{x\mid x\leqslant a,x\in L\}$，$T_2=\{x\mid x\geqslant a,x\in L\}$及$T_3=\{x\mid a\leqslant x\leqslant b,x\in L\}$都是$L$的子格.

定义 18.2.3 设$\langle L;\vee,\wedge\rangle$及$\langle L';+,\cdot\rangle$是两个格，若存在$L$到$L'$的映射$\sigma$使得对于$\forall a,b\in L$，有：

$$\sigma(a\vee b)=\sigma(a)+\sigma(b),$$
$$\sigma(a\wedge b)=\sigma(a)\cdot\sigma(b),$$

则称σ为L到L'的**（格）同态（映射）**(lattice homomor-phism).

还可仿照前述各种代数结构给出格的单同态、满同态、双同态（同构）以及自同态、自同构等概念.

定理 18.2.4 设格$\langle L;\vee,\wedge\rangle$及格$\langle L';+,\cdot\rangle$在映射$\sigma$下同态，则此同态必能**保持顺序**(order preserving)，即若$a,b\in L$且$a\leqslant b$，则$\sigma(a)\leqslant'\sigma(b)$，这里的$\leqslant$及$\leqslant'$分别是$L$及$L'$中的偏序关系.

例 18.2.5 设集$A=\{a,b\}$，它的幂集$\mathscr{P}(A)=$

$\{\varnothing,\{a\},\{b\},\{a,b\}\}$，则$\langle\mathscr{P}(A);\cup,\cap\rangle$是格. 另设 $B=\{0,1\}$，则 $B^2=\{(0,0),(0,1),(1,0),(1,1)\}$，并规定$(a_1,a_2)\vee(b_1,b_2)=(c_1,c_2)$，其中 $c_1=a_1\vee b_1$，$c_2=a_2\vee b_2$，$(a_1,a_2)\wedge(b_1,b_2)=(d_1,d_2)$，其中 $d_1=a_1\wedge b_1$，$d_2=a_2\wedge b_2$. 可以证明$\langle B^2;\vee,\wedge\rangle$是格. 作 $\sigma:\mathscr{P}(A)\to B^2$，使

$$\sigma:\varnothing\mapsto(0,0),\{a\}\mapsto(0,1),\{b\}\mapsto(1,0),\{a,b\}\mapsto(1,1).$$

则 σ 是 $\mathscr{P}(A)$ 到 B^2 的同构映射.

18.3 格的分类

由格的定义，格的任意两个元都有最小上界和最大下界，利用数学归纳法可以证明，格的每个有限子格都有最小上界和最大下界，但对于格的无限子集当然不一定有这一性质. 对此给出以下定义.

定义 18.3.1 若格 L 的每个非空子集都有 sup 和 inf，则称它为**完全格**(complete lattice).

显然每个有限格都是完全格.

定义 18.3.2 (1) 若格 L 中存在零元"0"，能满足条件：

$$\forall x\in L\Rightarrow x\vee 0=x,$$

则称 0 是 L 的**零元**(zero element)或**泛下界**(universal lower bound).

(2) 若格 L 中存在元 1，能满足条件：

$$\forall x\in L\Rightarrow x\wedge 1=x.$$

则称 1 是 L 的**单元**(unity element)或**泛上界**(universal upper bound).

容易证明：若格 L 存在零元或单元，则它们必是唯一的.

例 18.3.3 (1) 设 $A=\{a,b,c\}$，则$\langle\mathscr{P}(A);\subseteq\rangle$的零元为$\varnothing$，

单元为 A.

(2) 在正整数集 $\mathbf{N}^+$ 关于整除关系 $a|b$ 所构成的格中，零元是正整数 1，无单元.

(3) 整数集 $\mathbf{Z}$ 关于数的大小关系"$\leqslant$"所构成的格 $\langle \mathbf{Z};\leqslant \rangle$ 中既无零元也无单元.

定义 18.3.4 有零元和单元的格，称为**有界格**(bounded lattice).

为突出有界性，有界格常记作 $\langle L;\vee,\wedge;0,1\rangle$.

定义 18.3.5 设 $\langle L;\vee,\wedge;0,1\rangle$ 是有界格，$x\in L$，若 $\exists y\in L$ 使得 $x\vee y=1$，$x\wedge y=0$，则称 y 是 x 的**补元**或 x 是 y 的**补元**(complement element). y 是 x 的补元用 $y=x'$ 表示.

一般而言，有界格中的元不一定有补元，即使有补元也不一定唯一.

定义 18.3.6 设 $\langle L;\vee,\wedge;0,1\rangle$ 为有界格，若其中每个元 a 至少有一个补元 a'，则称 $\langle L;\vee,\wedge;0,1\rangle$ 为**有补格** complemented lattice).

例 18.3.7 图 18.6 的格 L_1 是有补格，例如元 a 有三个补元 b,c,d，这是因为：

$a\vee b=1, a\wedge b=0$；

$a\vee c=1, a\wedge c=0$；

$a\vee d=1, a\wedge d=0$.

同理，其他各元也都如此. 此外，0、1 互为补元. 故 L_1 是有补格.

图 18.7 的格 L_2 也是有补格，因为它的每个元都有一个补元，如元 a 与 f 互为补元，元 c 与 d 互为补元，元 b 与 e 互为补元，0 与 1 互为补元，而且每个元的补元都是唯一的.

图 18.8 的格 L_3 不是有补格，如元 a 没有补元(元 b 有两个补

元 c 和 d).

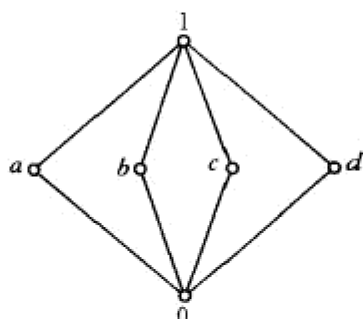


图 18.6

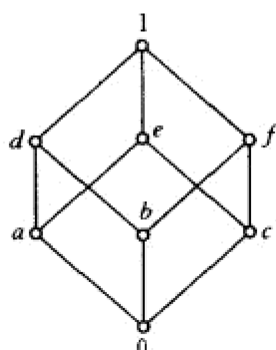


图 18.7

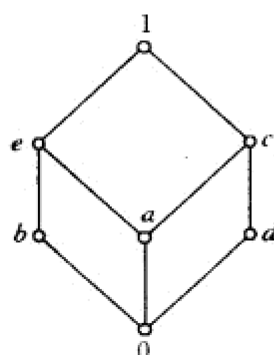


图 18.8

定义 18.3.8 设 $\langle L; \vee, \wedge \rangle$ 是格,若对于 $\forall x, y, z \in L$,以下二分配律成立:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z),$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$

则称 $\langle L; \vee, \wedge \rangle$ 为**分配格**(distributive lattice).

注:上述两个分配律是等价的,即由其中任一个可推导出另一个,因此只需引出其中一个即可. 这里将其并列是为了方便.

例 18.3.9 直接验证可知 Hasse 图 18.9 表示的格是分配格;而图 18.10 所示格不是分配格,其中的 a, b, c 三元不满足分配律,因为



图 18.9

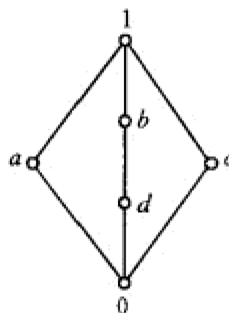


图 18.10

$$a\wedge(b\vee c)=a\wedge 1=a,$$
$$(a\wedge b)\vee(a\wedge c)=0\vee 0=0,$$
故
$$a\wedge(b\vee c)\neq(a\wedge b)\vee(a\wedge c).$$

定理 18.3.10 设 $\langle L;\vee,\wedge\rangle$ 是分配格，$a,x,y\in L$，若 $a\vee x=a\vee y$ 且 $a\wedge x=a\wedge y$，则 $x=y$. 特别地，若分配格 L 的元 a 有补元，则 a 的补元是唯一的.

定义 18.3.11 若格 L 既是有补格又是分配格，则称元为**布尔格**(Boole lattice).

注意 有补格仅保证每个元都有补元，但不保证补元的唯一性；分配格则保证若元 a 存在补元时，则补元必定唯一，但不保证补元的存在性. 而 Boole 格则同时具有此二性质.

18.4 Boole 代数的定义、例子及性质

布尔代数就是 Boole 格，它既可利用偏序关系定义，也可以利用运算来定义.

定义 18.4.1 有补分配格称为 **Boole 代数**(Boole algebra).

由于它的每个元 a 的补元 a' 唯一存在，而且 $(a')'=a$，所以可以把求补看作阶为 2 的一元运算. 以此与定义 18.1.10 的结果联合起来就可得到利用代数运算给出的 Boole 代数的另一定义.

定义 18.4.2 设 B 是集，在其上有两个二元运算 $\vee$ 与 $\wedge$（为了方便，按惯例改用＋与・表示）及一个一元运算“$'$”以及元 0 与 1. 若满足以下五组公理，则称 B 为 **Boole 代数**，记为 $B=\langle B;+,\cdot,{}';0,1\rangle$：

(1) 封闭性　$\forall x,y\in B, x+y, x\cdot y\in B$；

(2) 零元与单元的存在性

$$\exists 0\in B，对于\ \forall x\in B: x+0=x;$$
$$\exists 1\in B，对于\ \forall x\in B: x\cdot 1=x;$$

(3) 补元的存在性

$$\forall x \in B, \exists x' \in B: x + x' = 1, x \cdot x' = 0;$$

(4) 交换律　$\forall x, y \in B$,

$$x + y = y + x, x \cdot y = y \cdot x;$$

(5) 分配律　$\forall x, y, z \in B$:

$$x \cdot (y + z) = x \cdot y + x \cdot z,$$

$$x + (y \cdot z) = (x + y) \cdot (x + z).$$

例 18.4.3　(1) 在 18.1 节中已知集 X 的幂集 $\mathscr{P}(X)$ 关于 $\cup$、$\cap$, $'$ 构成格的简单例子. 现设 X 是任意集, $\mathscr{P}(X)$ 是它的幂集, 其零元及单元分别是空集 $\varnothing$ 及全集 X, 则 $\langle \mathscr{P}(X); t, \cdot, '; 0, 1 \rangle$ 构成布尔代数, 通常称之为 **X 的幂集代数**.

(2) 设 $B_2 = \{0, 1\}$, 三种运算如表 18.1 所示:

表　18.1

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

′	
0	1
1	0

直接验证可知它是 Boole 代数, 这种 Boole 代数也称为**二值代数**或**开关代数**.

(3) 设 S 是命题公式集, $\vee$, $\wedge$ 及 $\neg$ 分别表示命题 p, q 的析取 $(p \vee q)$, 合取 $(p \wedge q)$ 及命题 p 的否定 $(\neg p)$; 另用 T 表示恒真命题 $(p \to p)$, F 表示恒假命题 $(p \to \neg p)$, 则可证命题演算系统满足布尔代数的所有公理, 故也是布尔代数, 该代数称为**命题代数**或**公式代数**, 并用 $\langle S; \vee, \wedge, \neg; \mathrm{T}, \mathrm{F} \rangle$ 表示.

由于 Boole 代数是有补分配格, 所以它具有相应代数结构的性质, 为方便使用, 现将它所具有的运算性质及偏序性质罗列

如下：

定理 18.4.4 设$\langle B;+,\cdot,';0,1\rangle$是 Boole 代数，$\forall a,b,c\in B$,则它满足以下各法则：

(1) 幂等律 $a+a=a, a\cdot a=a$.

(2) 交换律 $a+b=b+a, a\cdot b=b\cdot a$.

(3) 结合律 $(a+b)+c=a+(b+c)$,

$(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

(4) 吸收律 $a+(a\cdot b)=a, a\cdot(a+b)=a$.

(5) 分配律 $a+(b\cdot c)=(a+b)\cdot(a+c)$,

$a\cdot(b+c)=(a\cdot b)+(a\cdot c)$.

(6) $(a\cdot b)+(b\cdot c)+(c\cdot a)=(a+b)\cdot(b+c)\cdot(c+a)$.

(7) 消去律

$$a+b=a+c, a\cdot b=a\cdot c\Rightarrow b=c.$$

(8) 有界性 $0\leqslant a\leqslant 1$.

(9) 0-1 律

$$a+0=a, a+1=1,$$
$$a\cdot 0=0, a\cdot 1=a.$$

(10) 互补律

$$a+a'=1, a\cdot a'=0,$$
$$0'=1, 1'=0.$$

(11) DeMorgan 律

$$(a+b)'=a'\cdot b', (a\cdot b)'=a'+b'.$$

(12) $a\leqslant b\Leftrightarrow a+b=b\Leftrightarrow a\cdot b=a$.

(13) $a+b=\sup(a,b), a\cdot b=\inf(a,b)$.

(14) $a\leqslant b\Leftrightarrow a\cdot b'=0\Leftrightarrow b'\leqslant a'\Leftrightarrow a'+b=1$.

(15) 对偶原理 对于 Boole 代数 B 中的等式，若对换其中的"+"与"·"，"0"与"1"，则所得结果仍为等式.

18.5 Boole代数的构造

与其他代数结构一样，在Boole代数中也要建立子Boole代数及Boole同态等概念，为了研究它的构造，这里还要引入原子的概念.

定义 18.5.1 设$\langle B;+,\cdot,';0,1\rangle$是Boole代数，$B_0$是$B$的子集，若$\langle B_0;+,\cdot,';0,1\rangle$本身是一个布尔代数，则称$B_0$是$B$的**子代数**(subalgebra). 换言之，B_0若有下列性质则构成B的子代数：

(1) $0,1\in B_0$；

(2) $x,y\in B_0\Rightarrow x+y,x\cdot y,x'\in B_0$.

注：这两个条件还可削弱成

(1) $B_0\neq\varnothing$；

(2) $x,y\in B_0\Rightarrow x+y,x'\in B_0$.

这是因为由$x+y$及$x'\in B_0$，利用DeMorgan律即可推得$x\cdot y\in B_0$.

定义 18.5.2 设$\langle B;+,\cdot,';0,1\rangle$及$\langle B^*;\vee,\wedge,-;0^*,1^*\rangle$是两个布尔代数，映射$\varphi\colon B\to B^*$称为(Boole)**同态**(Boole homomorphism)，如果它满足以下条件：

(1) $\varphi\colon 0\mapsto 0^*,1\mapsto 1^*$；

(2) $\forall x,y\in B,\varphi(x+y)=\varphi(x)\vee\varphi(y)$,

$$\varphi(x\cdot y)=\varphi(x)\wedge\varphi(y),$$

$$\varphi(x')=\overline{\varphi(x)}.$$

还可像其他代数结构一样给出单同态、满同态、同构、自同态、自同构等概念.

注：同态定义中的条件(2)亦可删去$\varphi(x\cdot y)=\varphi(x)\wedge\varphi(y)$而简化成

$\forall x,y \in B \quad \varphi(x+y)=\varphi(x) \vee \varphi(y)$ 及 $\varphi(x')=\overline{\varphi(x)}$.

例 18.5.3 (1) 在任一 Boole 代数 $\langle B;+,\cdot,';0,1\rangle$ 中,子集 $\{0,1\}$ 是它的子代数.

(2) 布尔代数 B 在同态映射 $\varphi: B \to B^*$ 下的象 $\varphi(B)$ 是 B 的同态象 B^* 的子代数.

(3) 设 $A=\{a\}$,其幂集为 $\mathscr{P}(A)=\{\varnothing,A\}$,$B=\langle \mathscr{P}(A);\cup,\cap,';\varnothing,A\rangle$ 是布尔代数,它与二值代数(例 18.4.3(2))同构,这只要作映射 $\sigma: \varnothing \mapsto 0, a \mapsto 1$ 即可看出.

为了研究布尔代数的构造,引入原子概念.

定义 18.5.4 设 $\langle B;+,\cdot,';0,1\rangle$ 是布尔代数,$a\in B$,若对于 $\forall x\in B$,有:

(1) $a\neq 0$,

(2) $x\cdot a=a$ 或 $x\cdot a=0$,

则称元 a 为 B 的**原子**(atom)(它们在 Hasse 图中是直接位于零元上方的元素).

例 18.5.5 例 18.1.9(3)中 110 的正整数因子集 $L=\{1,2,5,10,11,22,55,110\}$ 关于整除关系不仅构成格,而且构成 Boole 代数,此时其二元运算 $\vee,\wedge$ 是求二数的最大公约数(gcd)及最小公倍数(lcm),正整数 x 的补元 x' 则是 $\dfrac{100}{x}$,其 Hasse 图如图 18.5 所示.由图可见该布尔代数的原子是 2,5,11.

注:任意 Boole 代数不一定存在原子,这里仅限于讨论有原子的 Boole 代数.

定义 18.5.6 若对于布尔代数 $\langle B;+,\cdot,';0,1\rangle$ 的每个非零元 x 都有一个原子 $a\leqslant x$,则称 B 为**原子布尔代数**(atomic Boole algebra).

定理 18.5.7 任一有限 Boole 代数都是原子 Boole 代数.

利用原子可以将原子 Boole 代数(特别是有限布尔代数)的元

素表示出来，而且可以通过原子集的幂集看到有限 Boole 代数的构造.

定理 18.5.8 原子表示定理 设 $\langle B;+,\cdot,';0,1\rangle$ 是原子布尔代数，A 是它的原子集，令 $\pi(x)$ 为如下集合：

$$\pi(x)=\{a \mid a\in A \text{ 且 } a\leqslant x\},$$

则 $x=\sum\limits_{a\in\pi(x)}a$. 而且在不计较次序的情况下，$x$ 的这种原子和的表示法是唯一的.

例 18.5.9 在例 18.5.5 中，L 的原子是 2,5,11，L 的元用原子表示的式子是

$$10=2\vee 5=[2,5],$$
$$22=2\vee 11=[2,11],$$
$$55=5\vee 11=[5,11],$$
$$110=2\vee 5\vee 11=[2,5,11].$$

算符 $[a,b,c]$ 表示求 a,b,c 的最小公倍数.

作为定理 18.5.8 的推论有如下定理.

定理 18.5.10 原子 Boole 代数中所有原子的和等于它的最大元 1.

还可证明，任一有限 Boole 代数都与它的原子集的幂集代数同构. 其精确描述是：

定理 18.5.11 有限 Boole 代数的 Stone 表示定理 设 $\langle B;+,\cdot,';0,1\rangle$ 是有限 Boole 代数，A 是 B 的原子集，则 Boole 代数 B 到幂集代数 $\langle \mathscr{P}(A);\cup,\cap,-;\varnothing,A\rangle$ 的映射 $\pi:x\mapsto\pi(x)=\{a|a\in A \text{ 且 } a\leqslant x\}$ 是构成 B 与 $\mathscr{P}(A)$ 间的同构.

例 18.5.12 在例 18.5.5 与例 18.5.9 中，$L=\{1,2,5,10,11,22,55,110\}$，其原子集 $A=\{2,5,11\}$，其幂集 $\mathscr{P}(A)=\{\varnothing,\{2\},\{5\},\{11\},\{2,5\},\{2,11\},\{5,11\},A\}$. 作 L 到 $\mathscr{P}(A)$ 的映射如下：

$\sigma(1)=\varnothing,\sigma(2)=\{2\},\sigma(5)=\{5\},\sigma(11)=\{11\},\sigma(10)=\{2,5\},\sigma(22)=\{2,11\},\sigma(55)=\{5,11\},\sigma(110)=\{2,5,11\}$.

则可证明 σ 确是 L 到 $\mathscr{P}(A)$上的同构映射.

作为推论还有以下定理.

定理 18.5.13 (1) 每个有限 Boole 代数 B 的元数必为 2 的某个方幂 2^n,其中 n 是 B 的原子个数;

(2) 若两个 Boole 代数的元数相等,则它们必定同构.

对于一般 Boole 代数(不管它是否为原子布尔代数)有以下定理.

定理 18.5.14 Stone 表示定理　每个 Boole 代数都与一个集合代数同构.

以下讨论两类特殊的 Boole 代数:Boole 代数 B_{2^r} 及 B_2^r $(r\in\mathbf{N}^+)$.

(1) 由定理 18.5.13 知任一有限 Boole 代数的元数$=2^r$. 故最小的 Boole 代数是二值代数 B_2(例 18.4.3(2));比 B_2 稍大一点的 Boole 代数是 $B_4=\{0,1,\alpha,\beta\}$,其运算表如表 18.2:

表　18.2

+	0	1	α	β
0	0	1	α	β
1	1	1	1	1
α	α	1	α	1
β	β	1	1	β

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	α	0
β	0	β	0	β

x	x'
0	1
1	0
α	β
β	α

(2) 在 B_2 的基础上作 B_2 的 r 重积集 $B_2^r=\underbrace{B_2\times B_2\times\cdots\times B_2}_{r\text{个}}=\{(\beta_1,\beta_2,\cdots,\beta_r)\mid\beta_i=0,1\}$,并以它为基集,规定三种运算如下:

设$(\beta_1,\cdots,\beta_r),(\beta_1',\cdots,\beta_r')\in B_2^r$,规定

$$(\beta_1,\cdots,\beta_r)+(\beta'_1,\cdots,\beta'_r)=(\gamma_1,\cdots,\gamma_r),$$
$$(\beta_1,\cdots,\beta_r)\cdot(\beta'_1,\cdots,\beta'_r)=(\delta_1,\cdots,\delta_r),$$
$$(\beta_1,\cdots,\beta_r)'=(\beta'_1,\cdots,\beta'_r),$$

其中

$$\gamma_i=\max(\beta_i,\beta'_i),\delta_i=\min(\beta_i,\beta'_i),$$
$$\beta'_i=1-\beta_i.$$

经验证可知，B_2^r 关于这三种运算构成布尔代数 $\langle B_2^r;+,\cdot,';0,1\rangle$，其零元 0 及单元 1 分别是 $(0,\cdots,0)$ 及 $(1,\cdots,1)$.

关于以上两类代数有以下定理.

定理 18.5.15 Boole 代数 B_{2^r} 必与 B_2^r 同构，因而任意布尔代数必与某一 B_2^r 同构.

例 18.5.16 以 $B_4=\{0,\alpha,\beta,1\}$ 与 $B_2^2=\{(0,0),(0,1),(1,0),(1,1)\}$ 为例说明它们间的同构关系. 作映射

$$\sigma:0\mapsto(0,0),\alpha\mapsto(0,1),\beta\mapsto(1,0),1\mapsto(1,1),$$

即可知 σ 是一个同构映射，故 $B_4\overset{\sigma}{\cong}B_2^2$.

18.6 Boole 函数及其表达式

一般布尔代数 B 上的函数未必能用它上面的式子表示，但在二值 Boole 代数 $\langle B_2;+,\cdot,';0,1\rangle$ 中，它的每个从 B_2^n 到 B_2 的函数都能用包含 $+,\cdot,'$ 的表达式表示（二值 Boole 代数的完全性定理）. 为了简便，直接把布尔表达式作为 Boole 函数；在给出它的递归定义后将介绍范式定理，以便设计自动化设备时使用.

定义 18.6.1 设 $B=\langle B;+,\cdot,';0,1\rangle$ 是 Boole 代数，如下规定的表达式称为 B 上的 **Boole 函数**(Boole function)：

(1) 基集 B 中的元是 Boole 函数.

(2) 变量 $x_1,x_2,\cdots,x_n$ 是 Boole 函数.

(3) 若 f,g 是 Boole 函数，则 $f+g, f\cdot g, f', g'$ 也是 Boole 函数.

(4) 只有用(1)、(2)、(3)构成的表达式才是 Boole 函数.

例 18.6.2 (1) 在 Boole 代数 $B_4'=\langle\{0,1,\alpha,\beta\};+,\cdot,';0,1\rangle$ 中，1，$1+\alpha x_1+\beta x_2'$，$(\beta'+x_1+x_3)'$ 都是 Boole 函数.

(2) 在 B_4 上，$f(x,y)=(\beta x'y)+(\beta x(x+y')')+\alpha(x+x'y)$ 是 Boole 函数，它在 $x=\alpha, y=0$ 时的函数值是

$$\begin{aligned} f(\alpha,0)&=\beta\cdot\beta\cdot 0+(\beta\cdot\alpha(\alpha+1)')+\alpha(\alpha+(\beta\cdot 0)) \\ &=0+\beta\cdot\alpha\cdot 0+\alpha\cdot\alpha=\alpha. \end{aligned}$$

(3) 在 Boole 代数 $\langle B_2;+,\cdot,';0,1\rangle$ 上的两个 Boole 函数，$f(x,y,z)=xy+x'z+yz$ 及 $g(x,y,z)=xy+x'z$ 是相等的，这可通过函数值表(表 18.1)进行对比得到. 也可利用 18.4 节中的布尔代数公理及运算律作"恒等变形"来证明，其过程如下：

$$\begin{aligned} f(x,y,z)&=xy+x'z+(x+x')yz && \text{(互补律)} \\ &=(xy+xyz)+(x'z+x'yz) && \text{(交换律、结合律)} \\ &=xy(1+z)+x'z(1+z) && \text{(分配律)} \\ &=xy+x'z \quad \text{(0-1 律)} \\ &=g(x,y,z). \end{aligned}$$

表 18.3

x	y	z	$f(x,y,z)$	$g(x,y,z)$
0	0	0	0	0
0	0	1	1	1
0	1	0	0	0
0	1	1	1	1
1	0	0	0	0
1	0	1	0	0
1	1	0	1	1
1	1	1	1	1

定理 18.6.3 设$\langle B;+,\cdot,';0,1\rangle$是 Boole 代数，$F_n$ 是它上面的所有 n 元 Boole 函数的集，若规定 F_n 中任意两函数$f,g\in F_n$ 的三种运算如下：

$$(f+g)(x_1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)+g(x_1,x_2,\cdots,x_n),$$
$$(f\cdot g)(x_1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)\cdot g(x_1,x_2,\cdots,x_n),$$
$$f'(x_1,x_2,\cdots,x_n)=(f(x_1,x_2,\cdots,x_n))'.$$

则 F_n 关于这些运算构成一个含有 2^{2^n} 个元的 Boole 代数，其零元是恒取 0 值的函数，其单元是恒取 1 值的函数.

在 Boole 函数中有两种标准形式，即极小项范式（“析取范式”）及极大项范式（“合取范式”）.

定义 18.6.4 下列形式的 n 元 Boole 表达式

$$m_k=x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$$

称为 n 元**极小项**（minterm）或**基本合取式**（fundamental conjunctive form），其中 $\alpha_i\in\{0,1\}$，并规定

$$x_i^{\alpha_i}=\begin{cases}x_i',\text{当 }\alpha_i=0,\\ x_i,\text{当 }\alpha_i=1.\end{cases}$$

换言之，n 元极小项 m_k 是 n 个因子的乘积，其中第 i 个因子是 x_i 或 x_i'.

n 个变元的极小项共有 2^n 个，将它们记为 $m_0,m_1,m_2,\cdots,m_{2^n-1}$，通常用以下方法作极小项 m_k：先将下标 k 分别用十进制及二进制记数法表示，设

$$(k)_{10}=(\alpha_1\alpha_2\cdots\alpha_n)_2,$$

则

$$m_k=x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}.$$

现就 $n=1,2,3$ 写出所有的 n 元极小项如表 18.4～表 18.6.

表 18.4　$n=1, m_k$ 个数 $=2$

$(k)_{10}$	x	m_k
0	0	$m_0 = x'$
1	1	$m_1 = x$

表 18.5　$n=2, m_k$ 个数 $=4$

$(k)_{10}$	x_1	x_2	m_k
0	0	0	$m_0 = x'_1 x'_2$
1	0	1	$m_1 = x'_1 x_2$
2	1	0	$m_2 = x_1 x'_2$
3	1	1	$m_3 = x_1 x_2$

表 18.6　$n=3, m_k$ 个数 $=8$

$(k)_{10}$	x_1	x_2	x_3	m_k
0	0	0	0	$m_0 = x'_1 x'_2 x'_3$
1	0	0	1	$m_1 = x'_1 x'_2 x_3$
2	0	1	0	$m_2 = x'_1 x_2 x'_3$
3	0	1	1	$m_3 = x'_1 x_2 x_3$
4	1	0	0	$m_4 = x_1 x'_2 x'_3$
5	1	0	1	$m_5 = x_1 x'_2 x'_3$
6	1	1	0	$m_6 = x_1 x_2 x'_3$
7	1	1	1	$m_7 = x_1 x_2 x_3$

定理 18.6.5　极小项具有下列性质：

(1) 当 $i, j = 0, 1, \cdots, 2^n - 1$ 时

$$m_i \cdot m_j = \begin{cases} 0, i \neq j; \\ m_i, i = j. \end{cases}$$

（即两个不同的极小项之积为 0，两个相同的极小项之积为其本身.）

（2）$m_0 + m_1 + \cdots + m_{2^n-1} = 1$.

（即全部 n 元极小项之和为 1.）

由此可见，全体极小项$\{m_i\}$就是 Boole 代数 F_n 的原子（定义 18.5.4），据原子表示定理 18.5.8，F_n 的每个 Boole 函数都能用它们的和表示.

定义 18.6.6 一个或多个极小项相加的和式称为**极小项范式或析取范式**（minterm normal form/disjunctive normal form）.

定理 18.6.7 极小项范式定理 设 $B_2 = \langle B_2; +, \cdot, '; 0, 1\rangle$是二值布尔代数，则它的每个非零映射（函数）$f: B_2^n \to B_2$ 都能唯一地表示成极小项范式.

注：在本定理的叙述中引入了映射（函数）$f: B_2^n \to B_2$，并限制基础为二值 Boole 代数，这是为了使本定理的使用范围不局限于已由 Boole 表达式表示出的 Boole 函数，而可以是其他情况（如仅给出其对应规律或函数值表等）. 但就实际应用来说，二值 Boole 代数已足够了.

例 18.6.8 （1）简化 $f(x,y,z) = xy' + xz + y'z$ 为极小项范式.

解 此 Boole 表达式可用 18.4 节各公理及运算律将其变形成如下极小项范式：

$$\begin{aligned} f(x,y,z) &= xy'(z+z') + x(y+y')z + (x+x')y'z \\ &= xy'z + xy'z' + xyz + xy'z + xy'z + x'y'z \\ &= xy'z + xy'z' + xyz + x'y'z. \end{aligned}$$

(2) B_2 上的 Boole 函数 $f(x_1,x_2,x_3)$ 的函数值表如表 18.7，试求其极小项范式.

表 18.7

$(k)_{10}$	x_1	x_2	x_3	$f(x_1,x_2,x_3)$	m_k
0	0	0	0	0	
1	0	0	1	0	
2	0	1	0	1	$x_1'x_2x_3'$
3	0	1	1	0	
4	1	0	0	0	
5	1	0	1	1	$x_1x_2'x_3$
6	1	1	0	0	
7	1	1	1	0	

解 在函数值为 1 的各行(第 3,6 行)上写出相应的极小项 $m_2=x_1^0x_2^1x_3^0=x_1'x_2x_3'$ 及 $m_5=x_1^1x_2^0x_3^1=x_1x_2'x_3$，将它们相加即得到 $f(x_1,x_2,x_3)$ 的极小项范式

$$f(x_1,x_2,x_3)=x_1'x_2x_3'+x_1x_2'x_3.$$

经检验，该范式确是 $f(x_1,x_2,x_3)$ 的极小项范式：它仅在用表 18.7 的第 3 行及第 6 行上的二进制数 010 及 101 代入时方为 1，而用其余 6 行上的二进制数代入时则为 0，故符合要求.

一般地，每个最小项仅在用所在行首的二进制数代入时方为 1，而用其余数代入时则为 0.

由对偶原理，与极小项及其范式定理相应，布尔函数还有另一种标准形式.

定义 18.6.9 下列形式的 n 元 Boole 表达式

$$M_k=x_1^{\alpha_1}+x_2^{\alpha_2}+\cdots+x_n^{\alpha_n},$$

称为 n 元**极大项**(maxterm)或**基本析取式**(fundamental

disjunctive form)，其中 $\alpha_i \in \{0,1\}$，并规定

$$x_i^{\alpha_i} = \begin{cases} x_i, \text{当 } \alpha_i = 0, \\ x_i', \text{当 } \alpha_i = 1. \end{cases}$$

换言之，n 元极大项是 n 个变元的和，其中每个变元是 x_i 或 x_i'，若下标

$$(k)_{10} = (\alpha_1 \alpha_2 \cdots \alpha_n)_2,$$

则
$$M_k = x_1^{\alpha_1} + x_2^{\alpha_2} + \cdots + x_n^{\alpha_n}.$$

现仍就 $n=1,2,3$ 写出所有的 n 元极大项 M_k 如表 18.8～表 18.10.

表 18.8　$n=1, M_k$ 个数=2

$(k)_{10}$	x	M_k
0	0	$M_0 = x$
1	1	$M_1 = x'$

表 18.9　$n=2, M_k$ 个数=4

$(k)_{10}$	x_1	x_2	M_k
0	0	0	$M_0 = x_1 + x_2$
1	0	1	$M_1 = x_1 + x_2'$
2	1	0	$M_2 = x_1' + x_2$
3	1	1	$M_3 = x_1' + x_2'$

表 18.10　$n=3, M_k$ 个数=8

$(k)_{10}$	x_1	x_2	x_3	M_k
0	0	0	0	$M_0 = x_1 + x_2 + x_3$
1	0	0	1	$M_1 = x_1 + x_2 + x_3'$
2	0	1	0	$M_2 = x_1 + x_2' + x_3$
3	0	1	1	$M_3 = x_1 + x_2' + x_3'$
4	1	0	0	$M_4 = x_1' + x_2 + x_3$
5	1	0	1	$M_5 = x_1' + x_2 + x_3'$
6	1	1	0	$M_6 = x_1' + x_2' + x_3$
7	1	1	1	$M_7 = x_1' + x_2' + x_3'$

定义 18.6.10 一个或多个 n 元极大项的乘积称为**极大项范式**(maxterm normal form)或**合取范式**(conjunctive normal form).

定理 18.6.11 极大项范式定理 设$\langle B_2;+,\cdot,';0,1\rangle$是二值布尔代数,则它的每个不恒等于 1 的映射(函数)$f:B_2^n\to B_2$ 都能够唯一地表示成极大项范式.

例 18.6.12 求例 18.6.8(2)中 $f(x_1,x_2,x_3)$的极大项范式.

解 由对偶原理,此种范式应是函数值为 0 的 6 个行上的极大项的乘积,求得 $M_0=x_1+x_2+x_3$,$M_1=x_1+x_2+x_3'$,$M_3=x_1+x_2'+x_3'$,$M_4=x_1'+x_2+x_3$,$M_6=x_1'+x_2'+x_3$,$M_7=x_1'+x_2'+x_3'$,因而 $f(x_1,x_2,x_3)$的极大项范式是

$$
\begin{aligned}
M_0M_1M_3M_4M_6M_7=&(x_1+x_2+x_3)(x_1+x_2+x_3')\\
&\cdot(x_1+x_2'+x_3')\cdot(x_1'+x_2+x_3)\\
&\cdot(x_1'+x_2'+x_3)(x_1'+x_2'+x_3').
\end{aligned}
$$

18.7 Boole 函数的极小化

Boole 函数主要用于自动化电子线路的逻辑设计,由于 Boole 函数的形式多种多样,它们虽有相同的功能,却可以有不同的选择,本节只从经济的角度出发,研究 Boole 函数的极小化问题.

定义 18.7.1 将 Boole 代数 B 中的元及变元 $x_1,x_2,\cdots,x_n$,$a,b,\cdots$中的若干个相乘,然后将若干个这样的乘积相加所得的表达式称为**积和式**(product-sum # form)(或**与或式**(and-or form)).

例 18.7.2 (1) 每个极小项或每个极小项范式都是积和式.

(2) $x_1+x_2x_3'+x_1x_2x_3$,$abc+ab+abc'$,$da+cd+a'c+ab'cd$

都是积和式；而$(x+y)(x'+y)$，$(a+ab+abc)(a+b+c)$，$(ab+ab'+a'b)\cdot(a'b'+cd)$等都不是积和式.

定义 18.7.3 (1) 设 F 和 G 是两个相等的积和式，用 F_l，G_l 分别表示 F，G 中的记号（指 B 的元及变元）个数，用 F_s，G_s 分别表示它们的乘积项的个数. 若下列两不等式至少有一个是严格不等的，则称 G 较 F 简单：

$$G_l \leqslant F_l, G_s \leqslant F_s.$$

(2) 若在与 F 相等的所有积和式中，再也没有比 H 更简单的积和式时，就称 H 是**最简的**（或**最小的**）积和式.

化简积和式的方法有多种，如公式化简法、卡诺(Carlo)图化简法等等. 限于篇幅，这里仅介绍公式化简法. 它是使用一些公式将原式进行"恒等变形"以得到最简公式的方法，这里主要利用 Boole 代数的基本性质及五个常用的化简公式：

(1) $xy+xy'=x$；

(2) $x+x'y=x+y$；

(3) $xy+x'z+yz=xy'+x'z$；

(4) $(xy'+x'y)'=x'y'+xy$；

(5) $(xy+x'z)'=xy'+x'z'$.

利用这些公式化简时常需适当进行并项或添加适当的项，下面举例说明这些技巧.

例 18.7.4 (1) 化简 $f=ad+ad'+ab+a'c+bd+aceg+b'eg+deg$.

解 $f=a(d+d')+ab+aceg+a'c+bd+b'eg+deg$

$=(a+ab+aceg)+a'c+bd+b'eg+deg$

（将第一，二项并项后集中含 a 的各项，以便为 a 所"吸收"）

$=(a+a'c)+(bd+b'eg+deg)$

$=(a+c)+bd+b'eg$　　（公式(2)、(3)）

$=a+c+bd+b'eg.$

(2) 化简 $f=ab+ac'+b'c+c'b+b'd+d'b+ade(g+h)$.

解 $f=a(b+c')+b'c+c'b+b'd+d'b+ade(g+h)$

$=[a(b'c)'+b'c]+c'b+b'd+d'b+ade(g+h)$

（DeMorgan 律）

$=a+b'c+c'b+b'd+d'b+ade(g+h)$　　（公式(2)）

$=[a+ade(g+h)]+b'c+c'b+b'd+d'b$

$=a+b'c+c'b+b'd+d'b$　　（吸收律）

$=a+b'c(d+d')+c'b+b'd+d'b(c+c')$　（互补律）

$=a+b'cd+b'cd'+c'b+b'd+d'bc+d'bc'$

$=a+(b'cd+b'd)+(b'cd'+d'bc)+(c'b+d'bc')$

$=a+b'd+cd'+bc'$　　（吸收律及公式(1)）

18.8 Boole 函数在电路设计中的应用

Boole 代数的应用极为广泛，其中最明显的是在自动化技术及计算机技术中的应用，此外在诸如人工智能、机器证明、数理逻辑、概率论、测度论、拓扑学、泛函分析中都有广泛的应用. 本节仅讨论开关代数在分析、综合、设计逻辑电路中的应用.

连接两个端点 T_1,T_2 的导线与开关的组合称为**开关网络**(switching-network)，用 $a,b,c,\cdots$ 表示开关，用 1,0 分别表示开关的“接通”和“断开”以及整个电路的“接通”和“断开”，则此网络上电路是否能接通完全取决于这些开关的状态（取 0 或取 1）及其连接方式（并联、串联或反相），因而是开关的函数，今用

$f(x_1,x_2,\cdots,x_n)$表示$\{0,1\}^n\to\{0,1\}$的开关函数，用 F_n 表示 n 元开关函数的集，则根据定理 18.6.3，$\langle F_n;+,\cdot,';0,1\rangle$ 构成一个布尔代数，在对电路进行分析、综合时可以使用布尔代数的理论.

18.8.1 开关电路的分析与综合

对电路进行分析是指找出电路接通和电路断开的条件；对自动化设备进行综合，则指根据所给条件来设计电路使能满足这些条件. 现举例说明.

例 18.8.1 电路分析 设电路图 18.11 已给出，要求找出它们接通和断开的条件；为此先根据电路图作出其构造式，然后利用函数值表(或其他方法)求出与各开关所处状态相应的函数值，使函数值取 1 者即为电路接通时各开关所处的状态.

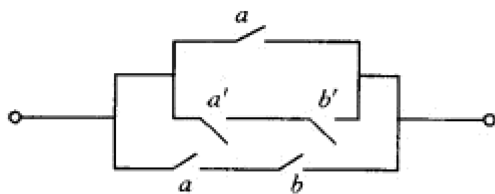


图 18.11

(1) 电路如图 18.11，试对它进行分析，找出其工作条件.

解 该电路的构造式是 $a+a'b'+ab$，为了便于分析，首先将它化简

$$\begin{aligned}(a+a'b')+ab &= (a+b')+ab\\ &= (a+ab)+b'\\ &= a+b'.\end{aligned}$$

作 $a+b'$的函数值表 18.11 即知该电流接通的电路是：

表 18.11

a	b	$a+b'$
0	0	1
0	1	0
1	0	1
1	1	1

1）$a=b=0$；

2）$a=1,b=0$；

3）$a=b=1$.

（2）电路如图 18.12，试分析其工作条件.

表 18.12

a	b	c	$f(a,b,c)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

解 图 18.12 的构造式是

$f(a,b,c)=ab+ac+bc$，作其函数值表 18.12，即知电路接通的条件是：

1）$a=0,b=c=1$；

2）$a=c=1,b=0$；

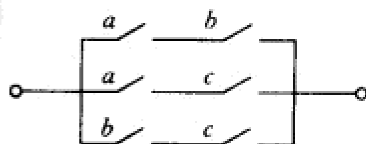


图 18.12

3) $a=b=1, c=0$;

4) $a=b=c=1$.

例 18.8.2 电路综合　下两题对设备提出了工作条件，要求设计电路使其满足所给条件，从开关函数观点看就是已知函数值，求出函数表达式. 可以利用 18.6 节求极小项范式(或"积和范式"、"与或范式")方法解决.

(1) 要设计一个为三人小组进行秘密表决的电路，要求信号在两人或两人以上按下开关表示同意时亮，其他情况不亮.

解　设三人各控制开关 a, b, c，根据题意作出开关函数 $f(a,b,c)$ 的函数值表及函数值取 1 的各行的极小项如表 18.13 所示，将各极小项相加即得该电路的积和范式

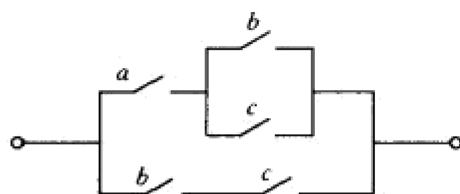


图　18.13

$$f(a,b,c)=a'bc+ab'c+abc'+abc.$$

将此式化简得

$$f(a,b,c)=a(b+c)+bc.$$

表　18.13

a	b	c	$f(a,b,c)$	m_k
0	0	0	0	
0	0	1	0	
0	1	0	0	
0	1	1	1	$m_3=a'bc$
1	0	0	0	
1	0	1	1	$m_5=ab'c$
1	1	0	1	$m_6=abc'$
1	1	1	1	$m_7=abc$

图 18.13 即为所求的电路图.

(2) 某火车站要设计一个自动调度电路，月台形状如图 18.14 所示，要求火车从箭头方向开进站，在 G 处有一信号灯，该灯亮时火车可以进站，P_1 表示命题"月台 I 空着"，P_2，P_3 同义；S_1、S_2 表示该处之信号灯开放绿灯，即允许火车通行；t_1，t_2 表示该处之转辙器已拨至允许转弯的位置.

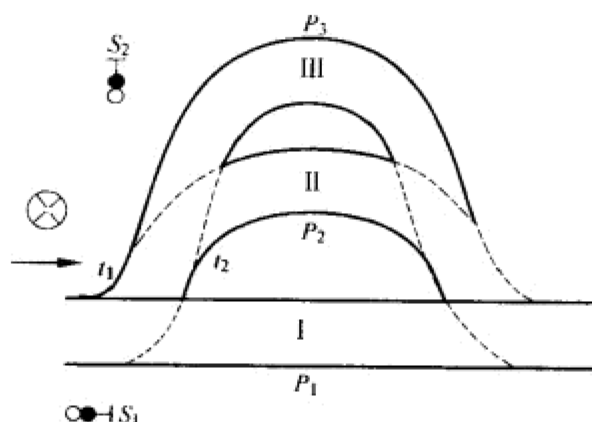


图 18.14

解 按照行车规定，火车可以进站的工作条件（容许进站时信号灯 G 亮）是下列三者之一：

1) $P_1=1, S_1=1, t_1=0$（此时可不考虑 P_2, P_3, S_2, t_2 的取值情况）；

2) $P_2=1, S_1=0, t_1=1, S_2=0, t_2=1$（此时可不考虑 P_1, P_3）；

3) $P_3=1, S_1=0, t_1=1, S_2=1, t_2=0$（此时可不考虑 P_1, P_2）.

把这些条件列一简化函数值表如表 18.14.

表 18.14

P_1	P_2	P_3	S_1	t_1	S_2	t_2	函数值	极小项
1			1	0			1	$P_1S_1t_1'$
	1		0	1	0	1	1	$P_2S_1't_1S_2't_2$
		1	0	1	1	0	1	$P_3S_1't_1S_2t_2'$

(不考虑的因素可不填入)相应的积和式是

$$F_G = P_1S_1t_1' + P_2S_1't_1S_2't_2 + P_3S_1't_1S_2t_2'.$$

化简得

$$F_G = P_1S_1t_1' + S_1't_1(P_2S_2't_2 + P_3S_2t_2').$$

其电路图如图 18.15.

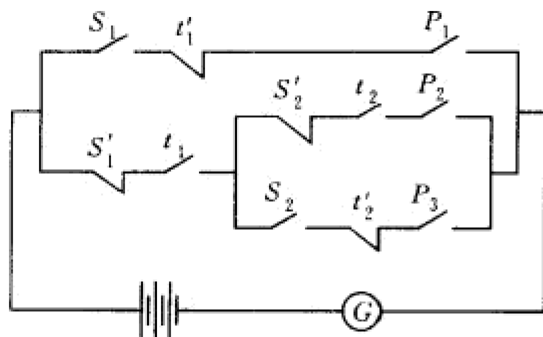


图 18.15

18.8.2 逻辑门电路

现把开关作为两种状态的器件来讨论,它是具有一个输入和一个输出的器件.对于多输入的情况可以用逻辑门来实现,它们可以用作"与"、"或"、"非"等逻辑运算,分别称它们为"与门"、"或门"和"非门",它们实际上是一种广义的开关,而"与"、"或"、"非"三种逻辑运算分别相当于布尔代数的"·","+","′"及开关代数的"串联"、"并联"及"反相".如果用变元 $a_1, a_2, \cdots$ 表示基本逻辑门的"输入",而用开关函数 f 表示门的"输出",则基本逻辑门可用布尔表达式与逻辑符号表示.由极小项范式定理,每个开关函数都可用"与"、"或"、"非"三种门实现(当然还可利用这三种基本门电路组成的"与非门"、"或非门"、"与或非门"等组合的电路实现,这要根据具体情况适当选用.)

图 18.16 是门电路的机能图.

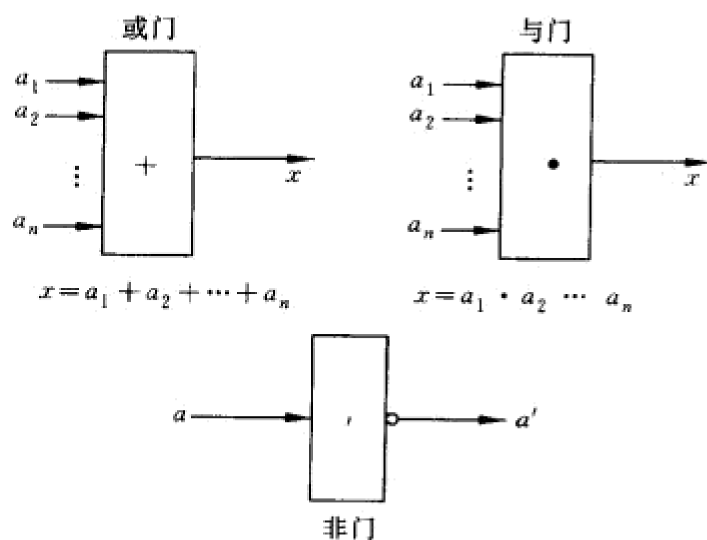


图 18.16

现以计算机的半加器的逻辑电路为例说明门电路的组合方式.

例 18.8.3 **半加器**(half adder) 能对两个一位的二进制数进行算术加法的自动装置称为**半加器**. 今假定 a 是被加数,b 是加数,x,y 分别是和 $a+b$ 的第二位及第一位的二进制数码,则有

$$\begin{array}{c}a\\ \underline{+b}\\ x\,y\end{array}\quad\begin{array}{c}0\\ \underline{+0}\\ 0\,0\end{array}\quad\begin{array}{c}0\\ \underline{+1}\\ 0\,1\end{array}\quad\begin{array}{c}1\\ \underline{+0}\\ 0\,1\end{array}\quad\begin{array}{c}1\\ \underline{+1}\\ 1\,0\end{array}.$$

此装置应有两个输出端分别输出 x 和 y. 作它们的函数值表 18.15 及表 18.16 如下:

表 18.15

a	b	x	m_k
0	0	0	
0	1	0	
1	0	0	
1	1	1	ab

表 18.16

a	b	y	m_k
0	0	0	
0	1	1	$a'b$
1	0	1	ab'
1	1	0	

其机能图如图 18.17.

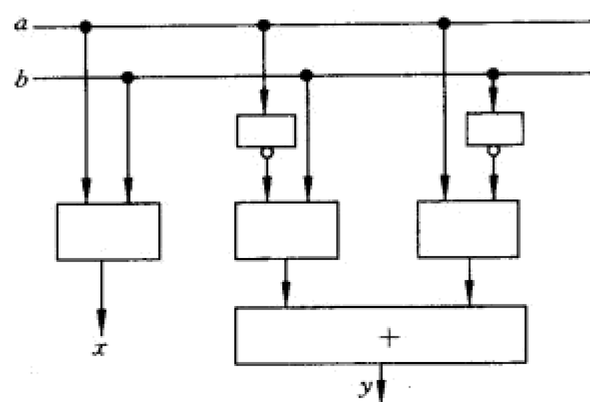


图 18.17

19 范畴与函子

前面已经讨论了群、环、域、模、格、代数等主要代数结构，下面将用更统一的观点，来研究各种代数结构的整体性质和宏观性质，给广泛存在于数学中的通用性、伴随性以简明而准确的描述.

数学范畴理论将各类数学结构(包括它们的“对象”和作用在所有对象间的“态射”)作为一个整体而形成所谓范畴，在范畴间用具有两种函数(“对象函数”和“态射函数”)功能的函子加以联系，然后在这些函子间用自然变换进行比较，因此它们间的关系较为复杂，层次较多，但可通过“交换图”来表示.

数学的范畴理论自 1945 年 Eilenberg. Maclane 在 Tran. Amer. Math. Soc 上发表奠基性文献“General Theory of Natural Equivalence”(自然等价的一般理论)以后，由于多数学者的努力，得到了迅速的发展，目前它的方法和结果已渗透到数学的很多分支并应用于形式语言、自动机理论及系统工程等领域并将应用于新近发展起来的突变理论(catastrophe theory)及混沌学理论(theory of chaos).

由于范畴理论牵涉面宽、层次较多，因此需要使用多种符号以免产生混乱，本书将使用花体字母 $\mathscr{C}$,$\mathscr{D}$ 等表示范畴，用大写拉丁字母 F,G 等表示函子，用小写字母 g、h 等表示态射(箭)，用小写希腊字母 η,ξ 等表示自然变换；此外当函子 F 作用到对象 A 上时表成 FA(不加括号). 而当函子 F 作用到态射 h,g 上时则加括号分别用 $F(h)$ 及 $F(g)$ 表示.

19.1 范畴的定义及例子

定义 19.1.1 **范畴**(category)$\mathscr{C}$由一个对象类和一个态射集$\mathscr{H}$组成,在$\mathscr{H}$中还规定了一个具有性质(4)、(5)、(6)的乘积,分别是:

(1) 对象(object)$A,B,C,\cdots$组成的**对象类**,记为 $\mathrm{ob}\mathscr{C}=\{A,B,C,\cdots\}$;

(2) $\mathscr{C}$的各对象间的**态射集** $\mathscr{H}=\{\hom_{\mathscr{C}}(A,B)\mid A,B\in \mathrm{ob}\mathscr{C}\}$,这里的 $\hom_{\mathscr{C}}(A,B)$是$\mathscr{C}$的对象 A 到对象 B 的一切映射 $f:A\to B$ 所构成的集,f 称为以 A 为定义域、以 B 为值域的**态射**(morphism)或**箭**(arrow);

(3) 态射的**乘积** 对于$\mathscr{C}$中的任意三个对象 A,B,C 有 $\hom_{\mathscr{C}}(A,B)\times\hom_{\mathscr{C}}(B,C)$到 $\hom_{\mathscr{C}}(A,C)$的映射:

$h:(f,g)\mapsto gf,$

这里 $f\in\hom_{\mathscr{C}}(A,B),g\in\hom_{\mathscr{C}}(B,C),h\in\hom_{\mathscr{C}}(A,C)$,$h$ 称为态射 f,g 的**乘积**;表示为 $h=g\cdot f$,简记为 $h=gf$.

(4) 态射的**不相重性** 若对象对$(A,B)\neq(C,D)$,则 $\hom_{\mathscr{C}}(A,B)\neq\hom_{\mathscr{C}}(C,D)$;

(5) 态射乘积的**结合性** 若 $f\in\hom_{\mathscr{C}}(A,B),g\in\hom_{\mathscr{C}}(B,C),h\in\hom_{\mathscr{C}}(C,D)$,则$(hg)f=h(gf)$,因此可将这个乘积简写为 hgf,它的定义域是 A,值域是 D,即 $hgf\in\hom_{\mathscr{C}}(A,D)$;

(6) 恒等态射的存在性 对于每个对象 A,存在一个 $1_A\in\hom(A,A)$使得对于每个 $f\in\hom_{\mathscr{C}}(A,B)$有 $f1_A=f$,而对于每个 $g\in\hom_{\mathscr{C}}(B,A)$,有 $1_Ag=g$(可证 1_A 是唯一的).

注 19.1.2 关于范畴定义的几点说明:

(1) 由集合构成的集称为类(class),比如说所有的群作为一个类,而每个群就是该类中的一个对象;同理对于其他代数结构也

是如此. 我们把全体对象称为“**对象类**”,而把各个对象间的全体态射称为“态射集”.

(2) 以前各章代数结构中曾谈到两个代数结构间的态射、同态、同构等,它们都是指“能保持代数运算的”映射,而本定义中的态射(或箭)则泛指能适合条件(4),(5),(6)的任何映射.

(3) 为了简便,在不引起误解的情况下,态射集符号的下标$\mathscr{C}$,$\mathscr{D}$,…常常省去,如$\hom_{\mathscr{C}}(A,B)$可省写成$\hom(A,B)$.

(4) 一个范畴中的关系常可用交换图(commutative diagram)表示,即用平面上的点表示对象,用$\overrightarrow{AB}$表示由A到B的态射,这样就构成一个平面有向图;如果从图的任一顶点出发,沿着图上的箭头方向经过有限步到达另一顶点,虽然走法不同但却到达同一顶点,这样的图就叫**交换图**. 图 19.1 是一个交换图,它表示态射h是f与g的乘积$h=gf$;图 19.2 表示$gf=kh$,图 19.3 则表示态射乘积的结合性:

$$h(gf)=(hg)f.$$

恒等态射1_A的存在性亦可用交换图表成图 19.4.

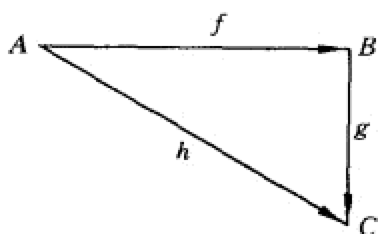


图 19.1

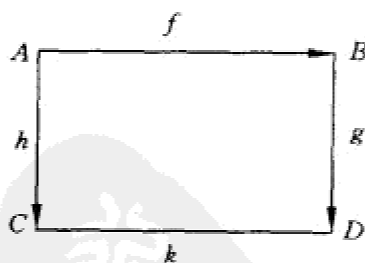


图 19.2

例 19.1.3 (1) 集范畴 Set:对象类是所有的集,态射集是集A到集B的映射集B^A,态射的“乘积”是映射的“复合”.

(2) 单元半群范畴 Mon: ob Mon 是所有的单元半群;$\hom(M,N)$是M到N的同态的集(M,N为单元半群);态射f,g

的乘法是同态 f 与 g 的复合 gf；恒等态射 1_M 是 M 上的恒等同态映射.

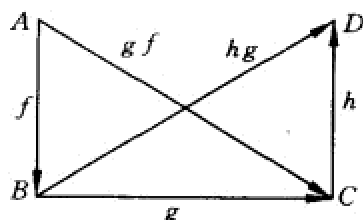


图 19.3

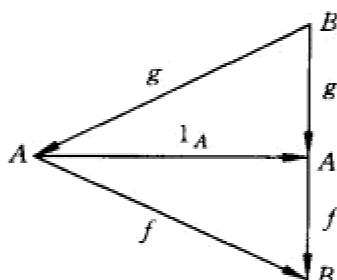


图 19.4

(3) 群范畴 Grp：ob Grp 是所有的群，其余与单元半群范畴类似.

(4) 交换群范畴 Ab：ob Ab 是所有的交换群，其余与单元半群范畴类似.

(5) 有单位元的（结合）环范畴 Ring：ob Ring 是所有有单位元 1 的环，态射集是将单位元 1 映入单位元 1 的一切环同态，态射乘法是环同态的乘法.

(6) 对是否含单位元 1 不作要求的（结合）环范畴 Rng： ob Rng 是所有结合环，态射集是一切环同态，态射乘法是环同态的乘法.

(7) 环 R 的左（右）模范畴 R-mod(mod-R)（这里的 R 为给定的环）： ob R-mod(ob mod-R) 是所有的左（右）R 模，态射集是一切 R-模同态，态射乘法是映射的复合；若 R 是一个除环则 R-mod(mod-R)是 R 上的左（右）向量空间范畴；若 R 是域，则构成 R 上的向量空间范畴 Vect.

(8) 拓扑空间范畴 Top： ob Top 是所有的拓扑空间；态射集是所有的连续映射；态射乘积是映射的合成.

下面介绍几个以前研究过的代数结构，可将它们视作特殊

范畴：

(9) 设 M 是单元半群，则可如下确定一个范畴 $\mathscr{M}$：使 $\mathrm{ob}\mathscr{M}=\{A\}$，即对象类仅含单独一个对象 A，并令 $\hom(A,A)=M$，而 1_A 是 M 的单位元. 对于 $\forall x,y\in\hom(A,A)$，规定态射 x,y 的乘积 xy 是 M 内元素 x 与元素 y 的乘积. 这样 $\mathscr{M}$ 就构成一个仅含单独一个对象的范畴. 反之，如果一个范畴仅含单独一个对象：$\mathrm{ob}\mathscr{M}=\{A\}$，则 $M=\hom\{A,A\}$ 是一个单元半群. 由于这些事实，则可将一个单元半群与对象类是单独一个对象的集范畴等同看待.

(10) 设 G 是一个群，同例(9)一样可作一个仅含单一对象的范畴 $\mathscr{G}$. 这个范畴的特点是仅含单独一个对象而且所有的态射都是同态映射.

19.2 某些基本的范畴概念

19.2.1 子范畴和小范畴

定义 19.2.1 设 $\mathscr{C},\mathscr{D}$ 是范畴，若 $\mathrm{ob}\mathscr{D}$ 是 $\mathrm{ob}\mathscr{C}$ 的子类($\mathrm{ob}\mathscr{D}\subseteq\mathrm{ob}\mathscr{C}$)，而且对于 $\forall A,B\in\mathrm{ob}\mathscr{D}$ 都有

$$\hom_{\mathscr{D}}(A,B)\subseteq\hom_{\mathscr{C}}(A,B).$$

此外 $\mathscr{D}$ 中态射的乘积以及每个对象 A 的恒等态射 1_A 也都与它在 $\mathscr{C}$ 中的相同，则称 $\mathscr{D}$ 为 $\mathscr{C}$ 的**子范畴**(subcategory).

定义 19.2.2 设 $\mathscr{D}$ 是 $\mathscr{C}$ 的子范畴，若对于 $\forall A,B\in\mathrm{ob}\mathscr{D}$ 都有

$$\hom_{\mathscr{D}}(A,B)=\hom_{\mathscr{C}}(A,B),$$

则称 $\mathscr{D}$ 为 $\mathscr{C}$ 的**完满子范畴**(full subcategory).

例 19.2.3 (1) Grp 及 Ab 都是 Mon 的完满子范畴，Ab 也是 Grp 的完满子范畴.

(2) Ring 是 Rng 的子范畴，但却不是它的完满子范畴，因为在有单位元的环中存在着能保持加法与乘法运算的映射，但它却

不能将 1 映射到 1.

(3) Mon, Grp 及 Ab 都不是 Set 的子范畴，因为它们不仅是集而且是具有二元运算及单位元的代数系统.

(4) 以有限集为对象、以集间的映射为态射的范畴是 Set 的子范畴.

定义 19.2.4 若范畴 $\mathscr{C}$ 的对象类 ob$\mathscr{C}$ 是一个集(而不是类)，则称 $\mathscr{C}$ 为**小范畴**(small category).

例 19.2.5 例 19.1.3 之(9)，(10)中的范畴都是小范畴.

19.2.2 对偶范畴与积范畴

下面介绍两种由老范畴作新范畴的方法：

定义 19.2.6 设 $\mathscr{C}$ 是给定的范畴，现作 $\mathscr{C}^{\circ}$ 如下：

(1) $\mathrm{ob}\mathscr{C}^{\circ}=\mathrm{ob}\mathscr{C}$，即 $\mathscr{C}^{\circ}$ 的对象类仍是 $\mathscr{C}$ 的对象类；

(2) 对于 $\forall A,B\in \mathrm{ob}\mathscr{C}^{\circ}$，$\hom_{\mathscr{C}^{\circ}}(A,B)=\hom_{\mathscr{C}}(B,A)$；

(3) 对于 $f^{\circ}\in \hom_{\mathscr{C}^{\circ}}(A,B)$，$g^{\circ}\in \hom_{\mathscr{C}^{\circ}}(B,C)$ 使 $g^{\circ}\cdot f^{\circ}=(f\cdot g)^{\circ}$；

(4) $\mathscr{C}^{\circ}$ 中的 1_A 同 $\mathscr{C}$ 中的 1_A.

则 $\mathscr{C}^{\circ}$ 构成一个范畴，称为 $\mathscr{C}$ 的**对偶范畴**(dual category).

由 $\mathscr{C}^{\circ}$ 的定义可知：由 $\mathscr{C}$ 的一个交换图(见图 19.5)可以得到 $\mathscr{C}^{\circ}$ 的对应的交换图，这时原图上的顶点及线均不必变化，只需改变图中各箭头的方向，因为 $\mathscr{C}$ 中的 $B\xrightarrow{g}A$ 是与 $\mathscr{C}^{\circ}$ 中的 $A\xrightarrow{g^{\circ}}B$ 相应的(余同).

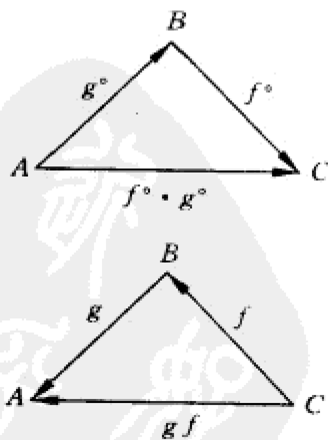


图 19.5

定义 19.2.7 设 $\mathscr{C}$，$\mathscr{D}$ 是两个范畴，构作 $\mathscr{C}\times\mathscr{D}$ 如下：

(1) $\mathrm{ob}\,\mathscr{C}\times\mathscr{D}=\mathrm{ob}\,\mathscr{C}\times\mathrm{ob}\,\mathscr{D}$;

(2) $\forall A,B\in\mathrm{ob}\,\mathscr{C}$ 及 $\forall A',B'\in\mathrm{ob}\,\mathscr{D}$,规定 $\hom_{\mathscr{C}\times\mathscr{D}}((A,A'),(B,B'))=\hom_{\mathscr{C}}(A,B)\times\hom_{\mathscr{D}}(A',B')$;

(3) 设 $f\in\hom_{\mathscr{C}}(A,B)$,$g\in\hom_{\mathscr{C}}(B,C)$,$f'\in\hom_{\mathscr{D}}(A',B')$ 及 $g'\in\hom_{\mathscr{D}}(B',C')$,规定

$$(g,g')\cdot(f,f')=(gf,g'f');$$

(4) 令 $1_{(A,A')}=(1_A,1_{A'})$.

则 $\mathscr{C}\times\mathscr{D}$ 构成一个范畴,称为 $\mathscr{C}$ 与 $\mathscr{D}$ 的**积范畴**(product category).

19.2.3 同构态射与等价对象

定义 19.2.8 设态射 $f\in\hom(A,B)$,若存在一个态射 $g\in\hom(B,A)$,使得 $fg=1_B$ 及 $gf=1_A$,则态射 f 称为**同构态射**(isomorphism).此时态射 g 是被 f 唯一确定的,称为 f 的**逆态射**(inverse morphism),用 f^{-1} 表示.

例 19.2.9 (1) 集范畴 Set 的同构态射是集合之间的双射.

(2) 群范畴 Grp 的同构态射是通常的群同构,即群的同态双射.

(3) 拓扑空间范畴 Top 的同构态射是同胚映射.

定理 19.2.10 (1) $(f^{-1})^{-1}=f$.

(2) 若 f,h 都是同构态射,且 fh 有定义,则 fh 也是同构态射,而且 $(fh)^{-1}=h^{-1}f^{-1}$.

(3) 范畴中的每一个恒等态射 1_A 都是同构态射.

定义 19.2.11 设 $A,B\in\mathrm{ob}\,\mathscr{C}$,若 $f\in\hom(A,B)$ 是一个同构态射,则称 A 与 B 为**等价对象**(equivalent objects).

定理 19.2.12 若 A 与 B 为等价对象,则对于 $\forall C\in\mathrm{ob}\,\mathscr{C}$,都可以建立 $\hom(A,C)$ 与 $\hom(B,C)$ 间的一一对应.

19.2.4 始对象与终对象

定义 19.2.13 (1) 设 $\mathscr{C}$ 是范畴，$I\in \mathrm{ob}\mathscr{C}$，若对于 $\forall A\in \mathrm{ob}\mathscr{C}$，$\hom(I,A)$ 都是仅含单独一个元素的集，则称 I 为 $\mathscr{C}$ 的**始对象**(initial object).

(2) 设 $\mathscr{C}$ 是范畴，$T\in \mathrm{ob}\mathscr{C}$，若对于 $\forall A\in \mathrm{ob}\mathscr{C}$ $\hom(A,T)$ 都是仅含单独一个元素的集，则称 T 是 $\mathscr{C}$ 的**终对象**(terminal object).

(3) 若 $Z\in \mathrm{ob}\mathscr{C}$ 既是始对象又是终对象，则称 Z 是 $\mathscr{C}$ 的一个**零对象**(null object).

例 19.2.14 (1) 在集范畴 Set 中空集 $\varnothing$ 是始对象但不是终对象；每个单元素集如 $\{a\}$ 是一个终对象而不是始对象. 可以证明，它没有零对象.

(2) 在范畴 Grp 和 Ab 中仅含一个元素的群 $\{0\}$（当群的复合运算是乘法时是 $\{1\}$）既是它们的始对象也是它们的终对象，因而是它们的零对象.

定理 19.2.15 (1) 若 A 是范畴 $\mathscr{C}$ 的一个始(终)[零]对象，则 A 是范畴 $\mathscr{C}^{\circ}$ 的一个终(始)[零]对象.

(2) 若范畴 $\mathscr{C}$ 有始(终)[零]对象，则各个始(终)[零]对象必是等价对象，因而从同构的观点看它们都是唯一的.

19.2.5 单态射与满态射

定义 19.2.16 设在范畴 $\mathscr{C}$ 内，$A,B\in \mathrm{ob}\mathscr{C}$，$f:A\to B$，$g:B\to A$，而且 $gf=1_A$，则态射 f 称为 g 的**截口**(section)，g 称为 f 的**收缩**(retraction).

定义 19.2.17 (1) 设 $\mathscr{C}$ 是范畴，$f:A\to B$ 是它的态射，若它是**左可消的**(left cancellable)，即由 $fg_1=fg_2$ 就有 $g_1=g_2$，则称 f

为**单态射**(monic morphism).

(2) 设 $\mathscr{C}$ 是范畴,$f:A\to B$ 是它的态射,若它是**右可消的**(right cancellable),即由 $g_1f=g_2f$ 就有 $g_1=g_2$,则称 f 为**满态射**(epic morphism).

注意 这里定义单、满态射的方法与集合中定义单、满映射以及各个代数系统的单、满态射有所不同:过去我们说映射 $f:A\to B$ 是单的当且仅当对于 $\forall a_1,a_2\in A$ 当 $a_1\neq a_2$ 时都有 $f(a_1)\neq f(a_2)$;而 f 是满的当且仅当 $f(A)=B$. 另外,我们可以证明,对于集合的映射来说这两种定义是等价的. 现在我们要问这种情形在范畴论中是否继续有效?

定理 19.2.18 在范畴 Grp、R-mod 及 mod-R 中,$f\in\hom(A,B)$是单(满)态射当且仅当映射 f 在它们的基集里是单(满)射.

定理 19.2.19 在环范畴 Ring 中,态射是单态射当且仅当它在基集里是单(同态)映射,但它的满态射却未必是满(同态)映射.

例 19.2.20 满态射不是满(同态)映射的例子. 考虑由整数环 $\mathbf{Z}$ 到有理数域 $\mathbf{Q}$ 的任一单同态 f,设 g,h 是 $\mathbf{Q}$ 到一个环 $\mathbf{R}$ 的同态映射则 $gf=hf$ 当且仅当它们在 $\mathbf{Z}$ 上的限制相等:$g|\mathbf{Z}=h|\mathbf{Z}$,由于 $\mathbf{Q}$ 的一个同态完全由它在 $\mathbf{Z}$ 上的限制确定,故由 $gf=hf$ 可推出 $g=h$,因而 f 是满态射,但 f 却显然不是满(同态)映射.

定理 19.2.21 (1) 设 $f:A\to B$ 及 $g:B\to C$ 且 f 及 g 都是单(满)态射,则 gf 也是单(满)态射.

(2) 设 $f:A\to B$ 及 $g:B\to C$ 而且 gf 是态射,则 f 也是单态射;若 gf 是满态射,则 g 也是满态射.

(3) 若 f 是一个截口,则 f 是满态射;若 f 是一个收缩,则 f 是一个单态射.

19.3 对偶原则

从以上两节可以看到范畴论中很多概念是成对出现的，如截口与收缩、始对象与终对象、单态射与满态射、范畴与对偶范畴等等；与它们有关的命题也都如此. 这是因为在范畴论中有一个"对偶原理".

定义 19.3.1 设 Σ 是由对象字母 $A,B,C,\cdots$ 态射字母 $f,g,h,\cdots$ 以及范畴名词、逻辑联结词、量词等组成的命题. 如果将 Σ 中的"定义域"与"值域"互换，"h 是 g 与 f 的乘积"与"h 是 f 与 g 的乘积"互换，而且将交换图中的箭头改变方向，"始对象"换成"终对象"，"终对象"换成"始对象"，"单射"换成"满射"，"满射"换成"单射"……而逻辑联结词及量词均不改变，由此得到的命题 Σ^* 称为 Σ 的**对偶命题**(dual statement).

例 19.3.2

<u>命题</u> Σ	<u>对偶命题</u> Σ^*
$f:A\to B$	$f:B\to A$
A 是定义域	A 是值域
$h=g\cdot f$	$h=f\cdot g$
f 是左可消的	f 是右可消的
f 是单态射	f 是满态射
A 是终对象	A 是始对象
Z 是零对象	Z 是零对象(因零对象是自对偶的)
定义：若态射 f 是左可消的，则称 f 为单态射.	定义：若态射 f 是右可消的，则称 f 为满态射.
定理　若 f 是一个截口，则 f 是满态射.	定理　若 f 是一个收缩，则 f 是单态射.

原理 19.3.3　对偶原则(duatity principle)　若命题 Σ 是一个对任何范畴都有意义的陈述句，则对偶命题 Σ^* 也是一个有意义的陈述句；若 Σ 是一个对任何范畴都成立的定理，则 Σ^* 也是一个定理.

注　该原则的依据是因为对偶范畴定义 19.2.6 的存在：因为 Σ 对一切范畴 $\mathscr{C}$ 成立，故 $\Sigma(\mathscr{C})$ 为真(或有意义). $\mathscr{C}^\circ$ 既是范畴，因而 $\Sigma(\mathscr{C}^\circ)$ 亦为真，将 $\mathscr{C}^\circ$ 用 $\mathscr{C}$ 的"语言"表示，则得到 $\mathscr{C}$ 对 Σ 的对偶命题 $\Sigma^*(\mathscr{C})$ 为真，现给出实例如下：

例 19.3.4　令 $\Sigma(\mathscr{C})$ 是命题"若由 $g_1 f = g_2 f$ 可得 $g_1 = g_2$，则 f 称为满态射"；

因 $\mathscr{C}^\circ$ 也是范畴，所以对它亦有意义：

$\Sigma(\mathscr{C}^\circ)$ 是命题"若由 $g_1^\circ f^\circ = g_2^\circ f^\circ$ 可得 $g_1^\circ = g_2^\circ$，则 f° 称为满态射"；

将 $\Sigma(\mathscr{C}^\circ)$ 用 $\mathscr{C}$ 中的语言表示，得 Σ 的对偶命题：

$\Sigma^*(\mathscr{C})$ 是命题"若由 $fg_1 = fg_2$ 可得 $g_1 = g_2$，则 f 称为单态射."

19.4　函子

定义 19.4.1　设 $\mathscr{C}$ 及 $\mathscr{D}$ 是两个范畴，满足下列条件的映射 F 称为由 $\mathscr{C}$ 到 $\mathscr{D}$ 的**(共变)函子**(covariant functor).

(1) F 是一个**对象函数**，F 是由 $\mathrm{ob}\mathscr{C}$ 到 $\mathrm{ob}\mathscr{D}$ 内的映射：

$$A \mapsto FA.$$

(2) F 是一个**态射函数**，即对于 $\mathscr{C}$ 的每一对象偶 (A,B)，F 将 $f \in \hom_{\mathscr{C}}(A,B)$ 映射到 $F(f) \in \hom_{\mathscr{D}}(FA,FB)$：

$$f \mapsto F(f).$$

(3) 若 gf 在 $\mathscr{C}$ 中有意义，则

$$F(gf) = F(g) \cdot F(f),$$

即二态射之积在映射 F 下的象恰是各态射在 F 下的象的积，亦即映射 F 能保持态射的乘法.

(4) $F(1_A)=1_{FA}$，

即映射 F 能保持恒等态射.

说明 (1) 函子亦可称为由范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的态射；

(2) 函子实际上由两个函数组成：一个是对象函数，一个是态射函数；

(3) 定义中的条件(3)可理解为由图 19.6 的可交换三角形经 F 映射成图 19.7 的可交换三角形：

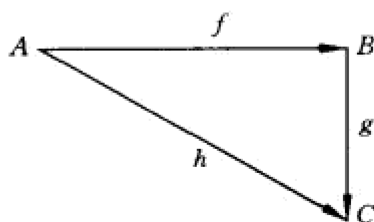


图 19.6

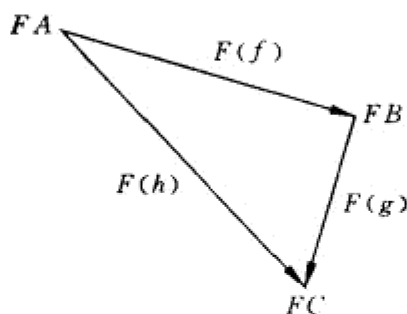


图 19.7

定义 19.4.2 (1) 由对偶范畴 $\mathscr{C}^{\circ}$ 到范畴 $\mathscr{D}$ 的函子称为 $\mathscr{C}$ 到 $\mathscr{D}$ 的**反变函子**(contravariant functor).

(2) 由积范畴 $\mathscr{B}\times\mathscr{C}$ 到范畴 $\mathscr{D}$ 的函子称为由范畴 $\mathscr{B}$ 及 $\mathscr{C}$ 到 $\mathscr{D}$ 的**双函子**(bifunctor).

说明 (1) $\mathscr{C}$ 到 $\mathscr{D}$ 的反变函子实际是一个映射 F，它能使 $\mathrm{ob}\mathscr{C}$ 映射到 $\mathrm{ob}\mathscr{D}$，对于每个对象偶 (A,B) 能将 $\hom(A,B)$ 映射到 $\hom(FB,FA)$；此外 F 使 $F(fg)=F(g)\cdot F(f)$ 及 $F(1_A)=1_{FA}$.

(2) 将双函子与反变函子结合起来可得到其他复杂的函子，如在 $\mathscr{B}$ 中为反变、在 $\mathscr{C}$ 中为共变的双函子 $\mathscr{B}^{\circ}\times\mathscr{C}$ 及在 $\mathscr{B},\mathscr{C}$ 中均为反变的双函子 $\mathscr{B}^{\circ}\times\mathscr{C}^{\circ}$ 等等.

例 19.4.3 (1) 设 $\mathscr{D}$ 是范畴 $\mathscr{C}$ 的子范畴，则 $\mathscr{D}$ 到 $\mathscr{C}$ 的、使 $\mathscr{D}$ 的每个对象 A 映射到($\mathscr{C}$ 的)对象 A、且使 $\mathscr{D}$ 的每个态射 f 映射到($\mathscr{C}$ 的)态射 f 的映射 F 作成一个由 $\mathscr{D}$ 到 $\mathscr{C}$ 的**单射函子**(injection functor).

(2) 由群范畴 Grp 到集范畴 Set 的函子 F：它是一个使群的对象类映射入群的基集，使群的同态射映入相应的映射的映射.

(3) 取任一单元环$\langle \mathbf{R};+,\cdot;0,1\rangle$，则它具有两种代数结构：加群$\langle \mathbf{R};+,0\rangle$及单元半群$\langle \mathbf{R};\cdot,1\rangle$，此外，一个环同态同时也是一个加群同态和一个单元半群同态，按照上述方法可得到由 Ring 到 Ab 的函子及由 Ring 到 Mon 的函子.

(4) 设 n 是正整数，作环 R 上的 n 阶矩阵环 $M_n(R)$，则由任一环同态 $f:R\to S$ 可确定一个由 $M_n(R)$ 到 $M_n(S)$ 的同态映射 $(r_{ij})\mapsto(f_{(r_{ij})})$，因而得到由 Ring 到 Ring 的函子 M_n.

(5) 条件同上，令 $\mathrm{GLn}(R)$ 表示 $M_n(R)$ 的单位所构成的群，即 R 上的所有 n 阶可逆方阵所成的群，映射 $R\mapsto \mathrm{GLn}(R)$ 及使 f 射入$(r_{ij}):(r_{ij})\mapsto(f_{(r_{ij})})$的映射复合成由 Ring 到 Grp 的函子 GLn.

(6) 集范畴 Set 中的**幂函子**(power functor)$\mathscr{P}$：此函子将每个集 A 映射到它的幂集 $\mathscr{P}(A)$，而将集映射 $f:A\to B$ 射入其诱导映射 $f_{\mathscr{P}}:\mathscr{P}(A)\mapsto\mathscr{P}(B)$.

(7) 群范畴 Grp 到 Ab 的交换化函子. 此函子 F 将任一群 G 映入交换群 $G/(G,G)$ 内，其中(G,G)是 G 的交换子群，即群 G 的交换子 $XYX^{-1}Y^{-1}(X,Y\in G)$的乘积所构成的正规子群. 设 f 是群 G 到群 H 的同态映射，因而 f 将(G,G)射入(H,H)，从而诱导出 $G/(G,G)$ 到 $H/(H,H)$ 的同态 $\overline{f}$，使 $F:f\mapsto\overline{f}$，则 $F:G\mapsto G/(G,G)$，$f\mapsto\overline{f}$ 就是所求的交换化函子.

(8) 偏序集范畴 Poset 是对象类为偏序集，而其态射集是它上面的保序映射构成的. 现作一左 R-模范畴 R-mod 到 Poset 的函子 F 如下：它将 R-mod$M$ 映射到 $L(M)$，后者是 M 的依包含关系

确定顺序的子模集；设 $f:M\to N$ 是一个模同态，则 f 亦确定一个由 $L(M)$ 到 $L(N)$ 中的保序映射 $\bar{f}$，使 $F:M\mapsto L(M)$，$f\mapsto\bar{f}$，则 F 也构成一个函子.

(9) 积范畴 $\mathscr{C}\times\mathscr{D}$ 到范畴 $\mathscr{C}$ 中的**射影函子**(projection functor)：它是将 $\mathscr{C}\times\mathscr{D}$ 的对象 (A,B) 映射到 $\mathscr{C}$ 的对象 A，将 $(f,g)\in\hom((A,B),(A',B'))$ 映射到 $f\in\hom(A,A)$ 的映射 $F:(A,B)\mapsto A,(f,g)\mapsto f$.

(10) 由范畴 $\mathscr{C}$ 到积范畴 $\mathscr{C}\times\mathscr{C}$ 的**对角线函子**(diagonal functor)系指映射 (f,f)，它使 A 映射到 (A,A)，而使 $f:A\to B$ 映射到 $\mathscr{C}\times\mathscr{C}$ 中的映射 (f,f)，这里 $(f,f):(A,A)\mapsto(B,B)$.

(11) 左 R-模范畴 R-mod 到右 R-模范畴 mod-R 的**对偶函子**(dual functor) D：对于每个左 R-模 M 按照左 R-模的方式作 M 到 R 内的同态集 $M^*=\hom_R(M,R)$，则可证 M^* 构成一个右 R-模. 因而可作 ob R-mod 到 ob mod-R 内的映射 $D:M\mapsto M^*$. 其次，为了确定 D 对于两个范畴间的态射的对应法则，可对 R-模 M 到 R-模 N 的同态 $L:M\to N$ 作转置映射 $L^*:N^*\to M^*$，这里 L^* 是由 g 与 L 的复合定义的(图 19.8)，即

$$L^*:g\mapsto gL.$$

令 $D:L\mapsto L^*$，则

$$D:M\mapsto M^*,L\mapsto L^*$$

构成一个对偶函子，它是反变函子.

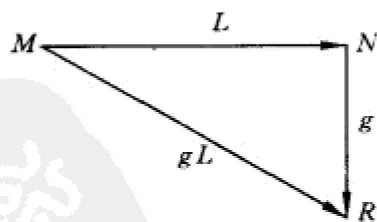


图 19.8

下面给出函子的几个简单性质.

定理 19.4.4 (1) 函子 F 使同构态射(定义 19.2.8)映射到同构态射，因而若二对象 A,B 等价(定义 19.2.11)，则 FA,FB 亦等价.

(2) 函子 F 使截口(收缩)(定义 19.2.16)映射到截口(收缩).

定义 19.4.5 设 F 是范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，若在 F 的映射下 $\mathscr{D}$ 的对象类丧失了 $\mathscr{C}$ 的对象类的全部或部分结构性质，$\mathscr{D}$ 的态射集也不能保持相应结构的运算性质，则此函子称为由 $\mathscr{C}$ 到 $\mathscr{D}$ 的**忘却函子**(forgetful functor).

例 19.4.6 在例 19.4.3(2)中，F 是由 Grp 到 Set 的函子，在 F 的作用下它们的对象类虽有相同的基集，它们的态射却是集的映射，但前者的群结构却在 Set 中被"忘却"了，故 F 是一个忘却函子. 又如例 19.4.3(3)的由 Ring 到 Ab 的函子"忘却"了前者的(乘法)单元半群结构，而由 Ring 到 Mon 的函子则"忘却"了环的加法群结构，因此二者都是忘却函子.

定义 19.4.7 设 F 是由范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，若对于 $\mathscr{C}$ 的每对对象 A,B 都能使 $\hom_{\mathscr{C}}(A,B)$ 到 $\hom_{\mathscr{D}}(FA,FB)$ 中的映射 $f\mapsto F(f)$ 是单射(满射)，则称 F 为**忠实(完满)函子**(faithful (full) functor).

例 19.4.8 例 19.4.3 (1) 由范畴 $\mathscr{C}$ 的子范畴 $\mathscr{D}$ 到 $\mathscr{C}$ 的单射函子是忠实函子；它是完满函子当且仅当 $\mathscr{D}$ 是 $\mathscr{C}$ 的完满子范畴.

例 19.4.3(2)、(3)的由 Grp 到 Set、由 Ring 到 Ab 及由 Ring 到 Mon 的函子都是忠实的，但却不是完满的.

例 19.4.3(9)由 $\mathscr{C}\times\mathscr{D}$ 到 $\mathscr{C}$ 的射影函子是完满的但却不是忠实的.

定义 19.4.9 设 F 是由 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，G 是由 $\mathscr{D}$ 到 $\mathscr{E}$ 的函子，则 F 与 G 的**复合 GF**(composite of functor)指的是由 $\mathscr{C}$ 到 $\mathscr{E}$ 的、具有如下性质的函子：

(1) 对于 $\forall A\in \mathrm{ob}\mathscr{C}$：$(GF)A=G(FA)$.

(2) 对于 $\forall f\in \hom_{\mathscr{C}}(A,B)$：$(GF)(f)=G(F(f))$.

例 19.4.10 例 19.4.3(5)是例(4)中的函子 M_n 与 Ring 到 Grp 的函子 U 的复合 U_{M_n}.

定理 19.4.11 若二函子 F,G 中一个是反变函子，另一个是

(共变)函子，则它们的复合 FG 是反变函子；若 F,G 都是反变函子，则 FG 是(共变)函子.

例 19.4.12 例 19.4.3(11)中的由 R-mod 到 mod-R 的对偶函子 D 是一个反变函子；将它使用两次就可得到由 R-mod 到它本身的(共变)函子.

19.5 自然变换

在两个范畴之间通常存在着许多个函子，这些函子之间又有一些映射联系着，本节将讨论广泛存在于数学领域(包括向量空间、矩阵、行列式、代数拓扑等)各函子间的一种"自然变换". 范畴理论的创始人 Eilenberg,MacLane 正是因为想给这种"自然性"以准确的含义才引入范畴和函子的.

定义 19.5.1 设 F 和 G 是 $\mathscr{C}$ 到 $\mathscr{D}$ 的两个函子，由 F 到 G 的**自然变换**(natural transformation)η 指的是一个映射，它给 $\mathscr{C}$ 的每个对象 A 指派一个态射 $\eta_A \in \hom_{\mathscr{D}}(FA,GA)$，使得对于 $\mathscr{C}$ 的任二对象 A,B 及任何 $f \in \hom_{\mathscr{C}}(A,B)$ 图 19.9 所示矩形是可换的.

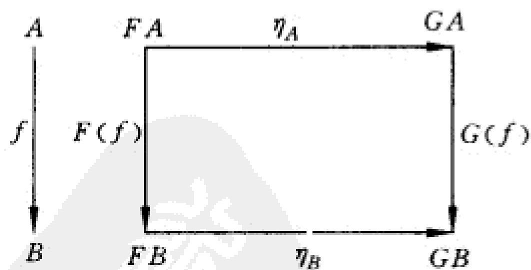


图 19.9

图中 $\eta_A(\eta_B)$ 称为自然变换 η 分别在 $A(B)$ 处的分量.

根据函子的定义(由对象函数及态射函数组成的一个能保持态射乘法及恒等态射的映射)可以把每个函子用 $\triangle ABC$(图

19.10)表示，自然变换 η 的作用是把这些三角形从 FA 平移到 GA.

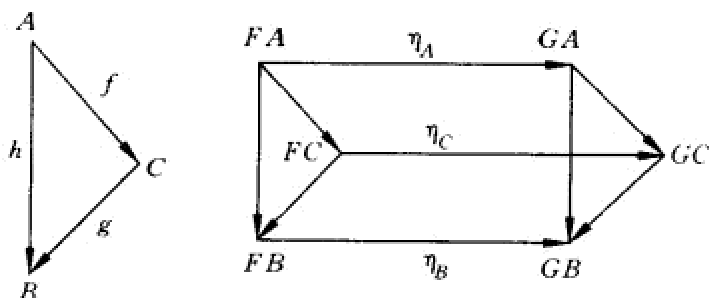


图 19.10

定义 19.5.2 若自然变换 η 的每个分量都是同构态射，则 η 称为**自然同构**(natural isomorphism).

例 19.5.3 (1) 设 K 是交换环，它上面的所有非奇异矩阵构成线性群 GLn(K)；此外每个环同态 $f:K\to K'$ 诱导出一个群同态 GLnf:GLn(K)→GLn(K'). 因而对于每个自然数 n 可以确定一个函子 GLn:CRng→Grp，这里 CRng 表示交换环范畴.

对于以上函子来说，从 $n\times n$ 矩阵 $\boldsymbol{M}$ 取行列式的变换 det 是一个自然变换：令 K^* 是交换环 K 的所有单位(即可逆元，见定理 15.4.6)所构成的群. 当行列式 $\det_k\boldsymbol{M}$ 是单位时，矩阵 $\boldsymbol{M}$ 是非奇异的而 $\det_k$ 是 GLn$K\to K^*$ 的一个群态射，即范畴 Grp 的一个态射. 由于行列式公式对一切环 K 有效，由交换环的每个态射 $f:K\to K'$ 都可得出一个交换图(图 19.11).

因而变换 det:GLn$f\to f^*$ 是 CRng→Grp 的两个函子间的自然变换.

(2) 例 19.4.3(7)的交换化函子，它当然可看成是由 Grp 到 Grp 的函子，现设 ν_G 表示 G 到其商群 $G/(G,G)$ 上的自然同态(定理 14.11.6)则得交换图(图 19.12).

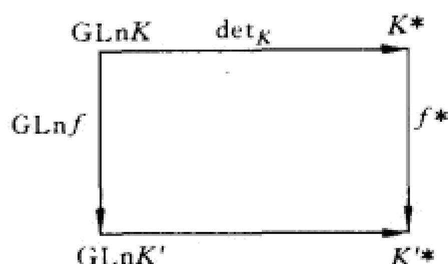


图 19.11

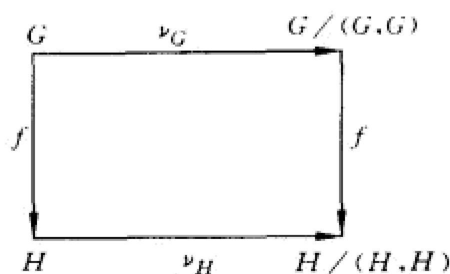


图 19.12

这就证明了映射 $\nu: G \mapsto \nu_G$ 是由 Grp 到 Grp 的恒等函子到交换化函子的自然变换.

(3) 在模范畴 R-mod 中,定义函子$\oplus_n$ 如下:它将模 M 映射到它的 n 重直和 $M^{(n)}$ 而将同态 $f: M \to N$ 映射到 $f^{(n)}$,

$$f^{(n)}: (a_1, \cdots, a_n) \mapsto (f(a_1), \cdots, f(a_n)),$$

则可证它是一个函子.

现对任意 M 作对角线同态:

$$\delta_M{}^{(n)}: a \mapsto \underbrace{(a, \cdots, a)}_{n\text{个}},$$

则映射 $\delta^{(n)}: M \mapsto \delta_M{}^{(n)}$ 是 R-mod 到$\oplus_n$ 的自然变换,这由交换图(图 19.13)可见.

与一般变换理论一样,对于自然变换也需要考虑它们的乘积、恒等自然变换及逆变换等,现介绍如下.

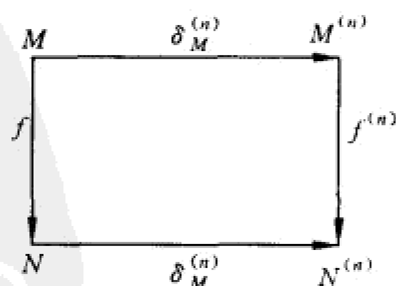


图 19.13

定义 19.5.4 设 F, G, H 是由范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的三个函子,η 是 F 到 G 的自然变换,ξ 是 G 到 H 的自然变换,设 $A \in \mathrm{ob}\mathscr{C}$,则 $\eta_A \in \hom_{\mathscr{D}}(FA, GA)$,$\xi_A \in \hom_{\mathscr{D}}(GA, HA)$,因而 $\xi_A\eta_A \in \hom_{\mathscr{D}}(FA, HA)$且符合由 F

到 H 的自然变换的可交换条件，即由图 19.14 所示的两个小交换图（即由顶点 FA,GA,GB,FB 构成的矩形与由 GA,HA,HB,GB 构成的矩形）可得到以 FA,HA,FB,HB 为顶点的大矩形也是一个交换图（图 19.14）的结论.

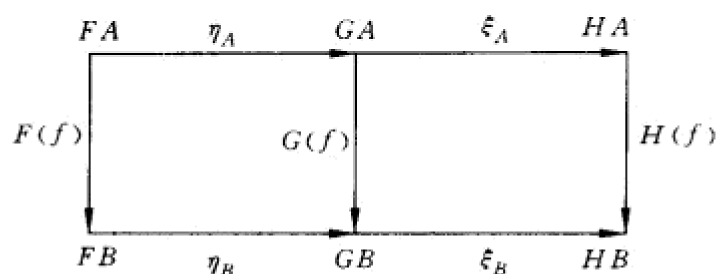


图 19.14

因而映射 $A \mapsto \xi_A \eta_A$ 是由 F 到 H 的自然变换，称自然变换 $\xi\eta$ 为自然变换 ξ 及 η 的**乘积**(product).

定义 19.5.5 设 F 是范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的一个函子，则可得到由 F 射入本身的一个自然变换 1_F，它将任意 $A \in \mathrm{ob}\mathscr{C}$ 射入态射 $1_{FA} \in \mathrm{hom}_{\mathscr{D}}(FA,FA)$. 设 G 是另一个由 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，η 是任一个由 F 到 G 的自然变换，则 $\eta 1_F = \eta = 1_G \eta$. 这样的 1_F 及 1_G 均称为**恒等自然变换**(identity natural transformation).

定义 19.5.6 设 η 是 F 到 G 的自然同构，则对于 $\forall A \in \mathrm{ob}\mathscr{C}$，$\eta_A : FA \to GA$ 是一个同构，从而有逆同构 $\eta_A^{-1} : GA \to FA$. 它显然满足自然变换的交换性，因而 $A \mapsto \eta_A^{-1}$ 是 G 到 F 的自然同构，称之为 **η 的逆自然变换**(inverse natural transformation)，用 η^{-1} 表示，显然有

(1) $\eta^{-1}\eta = 1_F, \eta\eta^{-1} = 1_G$;

(2) $(\eta^{-1})_A = \eta_A^{-1}$;

(3) $(\eta^{-1})^{-1} = \eta$;

(4) 若 η 是由 F 到 G 的自然变换，ζ 是由 G 到 F 的自然变换，

而且 $\zeta\eta=1_F$，$\eta\zeta=1_G$，则 η 是具有 $\eta^{-1}=\zeta$ 的自然同构.

19.6 范畴的等价

定义 19.6.1 设 $\mathscr{C}$ 及 $\mathscr{D}$ 是两个范畴，如果存在函子 $F:\mathscr{C}\to\mathscr{D}$ 及 $G:\mathscr{D}\to\mathscr{C}$ 使得 $GF=1_{\mathscr{C}}$ 及 $FG=1_{\mathscr{D}}$，则称 $\mathscr{C}$ 与 $\mathscr{D}$ 是**同构范畴**(isomorphic category)，用 $\mathscr{C}\cong\mathscr{D}$ 表示.

例 19.6.2 (1) 范畴 Ab 与 $\mathbf{Z}$-mod 同构：设 M 是一个交换(加法)群，若规定 $nx(n\in\mathbf{Z},x\in\mathbf{M})$ 为 x 的 n 倍，则 M 可构成一个 $\mathbf{Z}$-mod；反之，若 M 是 $\mathbf{Z}$-mod，则其加群是一个加法交换群. 这样就有了互逆的由 ob Ab 到 ob $\mathbf{Z}$-mod 的及由 ob $\mathbf{Z}$-mod 到 ob Ab 的映射. 今设 f 是交换群 M 到交换群 N 的任一(群)同态，因 $f(nx)=nf(x)$，$(n\in\mathbf{Z},x\in M)$，则 f 是(作为 $\mathbf{Z}$-mod 的)M 到 N 的(群)同态；反之，任一模同态也是一个群同态，因此 Ab 与 $\mathbf{Z}$-mod是同构范畴.

(2) 范畴 R-mod 与 mod-R^{op} 同构，这里 R 是任意环：若 M 是一个左模，则可将它作成一个右 R^{op}-模，这只要对于 $x\in M,r\in R^{op}=R$(看作集合)规定 $xr=rx$ 就行了；若将此法倒转，则可将一右 R^{op}-模变成一个左模. 此外(作为左 R-模的)${}_RM$ 到 ${}_RN$ 的任一同态也是(作为右 R^{op}-模的)$M_{R^{op}}$ 到 $N_{R^{op}}$ 内的同态，这样就有了两个函子 F 及 G 能使 $GF=1_{R\text{-mod}}$ 及 $FG=1_{\text{mod-}R^{op}}$.

故 R-mod$\cong$mod-R^{op}.

两个同构的范畴完全可以看成相同的范畴，这样要求范畴的等同是过于严格了. 有时可将条件放宽成为范畴的等价.

定义 19.6.3 设 $\mathscr{C}$ 及 $\mathscr{D}$ 是两个范畴，如果存在函子 $F:\mathscr{C}\to\mathscr{D}$ 及 $G:\mathscr{D}\to\mathscr{C}$ 使 $GF\overset{n}{\cong}1_{\mathscr{C}}$ 及 $FG\overset{n}{\cong}1_{\mathscr{D}}$($\overset{n}{\cong}$表示函子的自然同构)，则称 $\mathscr{C}$ 与 $\mathscr{D}$ 为**等价范畴**(equivalent category)，并用(F,G)表示函子 F,

G 给出的等价关系.

由定义可见：

(1) 同构范畴必是等价范畴；

(2) 范畴的等价是一个等价关系.

可利用以下定理判定二范畴是否等价.

定理 19.6.4 设 F 是由范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，则存在函子 $G: D \to \mathscr{C}$ 使得 (F,G) 给出 $\mathscr{C}$ 与 $\mathscr{D}$ 等价关系的充要条件是：

(1) F 是一个忠实且完满的函子；

(2) 对于 $\mathscr{D}$ 的每一个对象 A' 存在 $\mathscr{C}$ 的一个对象 A，使 FA 及 A' 在 $\mathscr{D}$ 中是同构的（即有一同构包含于 $\hom_{\mathscr{D}}(FA,A')$ 之中）.

例 19.6.5 设 R 是环，$M_n(R)$ 是 R 上的 n 阶矩阵环，则 R 上的右模范畴 mod-R 与 $M_n(R)$ 上的右模范畴 mod-$M_n(R)$ 等价.

19.7 积与上积

很多数学结构（如集的乘积、群的直积、群的自由积等），一旦利用映射时就可以得到简单的描述. 范畴论是使用态射（箭）作为主要工具研究问题的，因而以上结构可以自然地纳入范畴论研究的范围.

定义 19.7.1 设 A_1, A_2 是范畴 $\mathscr{C}$ 的两个对象，则 A_1 与 A_2 的积，$A_1 \prod A_2$，是三元组 $\langle A; p_1, p_2\rangle$，其中 $A \in \mathrm{ob}\mathscr{C}$，$p_i \in \hom_{\mathscr{C}}(A, A_i)(i=1,2)$，它们满足以下条件：设 B 是 $\mathscr{C}$ 的任一对象，$f_i \in \hom_{\mathscr{C}}(B, A_i)(i=1,2)$，则存在唯一的 $f \in \hom_{\mathscr{C}}(B,A)$ 使得图 19.15 为交换图：

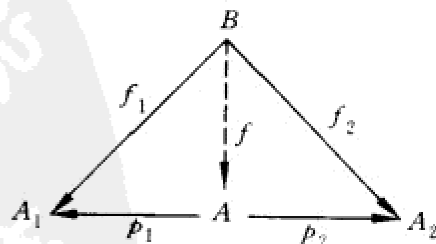


图 19.15

例 19.7.2 设 G_1, G_2 是两个

群，作积集 $G=G_1\times G_2=\{(g_1,g_2)\mid g_i\in G_i,i=1,2\}$，规定 G 的乘法为 $(g_1,g_2)(h_1,h_2)=(g_1h_1,g_2h_2)$，则 G 构成一个群，它的单元 $1=(1_1,1_2)$，其中 $1_1,1_2$ 分别是 G_1,G_2 的单元；逆元 $(g_1,g_2)^{-1}=(g_1^{-1},g_2^{-1})$.

作 G 到 G_i 中的射影 $p_i:G\to G_i(i=1,2)$，如下：

$$p_1:(g_1,g_2)\mapsto g_1,p_2:(g_1,g_2)\mapsto g_2,$$

则 p_1,p_2 分别是 G 到 G_1,G_2 的群同态.

任取 H 是另一群且设 $f_i:H\to G_i$ 是由 H 到 G_i 中的群同态，则可确定一个由 H 到 $G=G_1\times G_2$ 的映射 $f:h\mapsto(f_1(h),f_2(h))$，它显然是一个群同态且 $p_if(h)=f_i(h)$，因而得交换图 19.16. 所以三元组 $\langle G=G_1\times G;p_1,p_2\rangle$ 是群范畴 Grp 中两对象 G_1,G_2 的积.

定理 19.7.3 设 $\langle A_1;p_1,p_2\rangle$ 及 $\langle A_2;p_1',p_2'\rangle$ 是 $\mathscr{C}$ 的对象 A_1，A_2 的两个积，则必存在唯一的同构 $h:A_1\to A_2$ 使得 $p_i=p_i'h(i=1,2)$，即（从同构的观点看）A_1,A_2 的积是唯一的.

由于这种唯一性，我们才使用记号 $A_1\coprod A_2$ 表示 A_1 与 A_2 的积.

可以将两对象的积推广到多个对象的积.

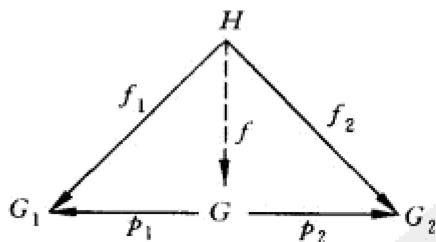


图 19.16

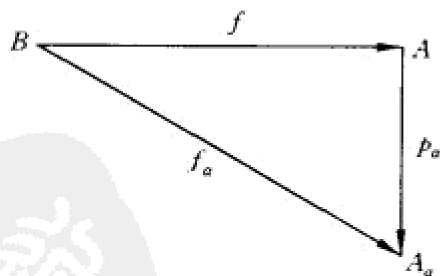


图 19.17

定义 19.7.4 设 $\{A_\alpha\mid\alpha\in I\}$ 是范畴 $\mathscr{C}$ 的对象的标号集，它们的积 $\prod A_\alpha$ 是一个集 $\{A;p_\alpha\mid\alpha\in I\}$，其中 $A\in\mathrm{ob}\mathscr{C}$，而 $p_\alpha\in$

$\hom_{\mathscr{C}}(A,A_\alpha)$，它们能使：若 $B\in \mathrm{ob}\mathscr{C}$ 且 $f_\alpha\in\hom_{\mathscr{C}}(B,A_\alpha)(\alpha\in I)$，则存在唯一的 $f\in\hom_{\mathscr{C}}(B,A)$ 使得每一个图都是交换的(图 19.17).

例 19.7.5 (1) 设$\{A_\alpha\mid\alpha\in I\}$是集的标号集，作积集 $A=\prod A_\alpha$ 为映射$a:I\to\bigcup A_\alpha$ 的集使对于每个$\alpha\in I$，$a(\alpha)=A_\alpha$. 对于每个α作射影 $p_\alpha:a\mapsto a(\alpha)$，则可证$\{A;p_\alpha\}$是范畴 Set 中各对象 A_α 的积.

(2) 设$\{G_\alpha\mid\alpha\in I\}$是群的标号集，在$G=\prod G_\alpha$ 中作积如下：对于 $g,g'\in G$ 使$gg'(\alpha)=g(\alpha)g'(\alpha)$，且使$G$的单元1由$1(\alpha)=1_\alpha$($1_\alpha$是$G_\alpha$的单元，$\alpha\in I$)确定. 易证这构成$G$上的一个群结构，而且同 Set 中一样，各射影都是同态，因而$\{G;p_\alpha\}$是群范畴中 G_α 的一个积.

(3) 以上作群标号集的积的方法和结论对环范畴 Ring 和 R-模范畴 R-mod 同样有效.

由对偶原则还可讨论积的对偶概念：上积.

定义 19.7.6 设$\{A_\alpha\mid\alpha\in I\}$是范畴$\mathscr{C}$的对象的一个标号集，它们的**上积**(coproduct)记作$\coprod A_\alpha$ 指的是集$\{A;i_\alpha\mid\alpha\in I\}$，其中 $A\in\mathrm{ob}\mathscr{C}$，而 $i_\alpha\in\hom(A_\alpha,A)$，它们能使：若 $B\in\mathrm{ob}\mathscr{C}$ 且 $g_\alpha\in\hom_{\mathscr{C}}(A_\alpha,B)(\alpha\in I)$，则存在唯一的 $g\in\hom_{\mathscr{C}}(A,B)$ 使每个图都是可交换的(图 19.18).

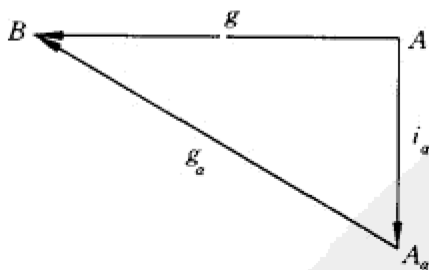


图 19.18

由对偶原理可得与定理 19.7.3 对偶的结论：范畴 $\mathscr{C}$ 的任一对象的标号集的上积如果存在，则它总是唯一的(在同构的意义上).

例 19.7.7 若$\{A_\alpha\mid\alpha\in I\}$是集的一个标号集，则必存在由各

集 A_α 的"不相交并"构成的集，记作 $\dot{\bigcup} A_\alpha$，令 i_α 表示 A_α 到 $\dot{\bigcup} A_\alpha$ 中的单映射，设 B 是一个集且设对每个 α 有 A_α 到 B 中的一个映射 g_α，则必存在 $\dot{\bigcup} A_\alpha$ 到 B 中的唯一映射 g 使得限制 $g \upharpoonright A_\alpha = g_\alpha(\alpha \in I)$，则可证 $\{\dot{\bigcup} A_\alpha; i_\alpha\}$ 是范畴 Set 内各 A_α 的上积.

定理 19.7.8 群范畴 Grp、环范畴 Ring、模范畴 R-mod 以及交换群范畴 Ab 的对象的任一标号集的上积必定存在.

19.8 核与上核

这是一对对偶的范畴概念，在群、环、模中都有同态核的概念，但由于范畴中的态射未必是同态，所以不能像群、环、模那样来定义态射的核，这可从下例看到：取所有对称群为对象、群同态为态射构成的范畴 $\mathscr{C}$ 内的 $f \in \hom(S_3, S_2)$（S_3 为三次对称群，S_2 为二次对称群）来看，则因

$f((1)) = f((1\ 2\ 3)) = f((1\ 3\ 2)) = (1) \in S_2$,

$f((1\ 2)) = f((1\ 3)) = f((2\ 3)) = (1\ 2) \in S_2$.

所以 $\ker f = N = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$，这是一个交代群 (alternate group)，$N \notin \mathrm{ob}\mathscr{C}$，由此可见在一般范畴中过去的同态核定义不再适用. 现从另一角度给出一般范畴的核的概念.

定义 19.8.1 设范畴 $\mathscr{C}$ 有零对象，因而有零态射；设 $f \in \hom(A, B)$，则态射 $g \in \hom(C, A)$ 称为 f 的核(kernel)，若它满足以下条件：

(1) g 是单态射；

(2) $fg = 0_{CB}$；

(3) 对于 $\forall h \in \hom(D, A)$，若 $fh = 0_{DB}$，则必有 $t \in \hom(D, C)$，使 $h = gt$，即其图是交换图 19.19.

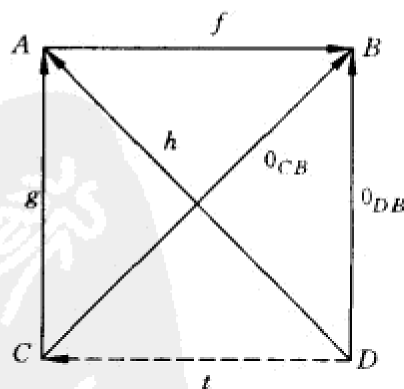


图 19.19

例 19.8.2 (1) 设 f 是群 G 到群 H 的同态，N 是 f 的同态核，则 $f(N)=0$，且 N 是 G 的正规子群，因而存在 N 到 G 的单同态 $g=1_G\upharpoonright N$(即 G 的恒等同态在 N 上的限制)，所以 $fg=0$. 此外，若有群 N_1 及 N_1 到 G 的同态 h 使 $fh(N_1)=0$，则 $h(N_1)\subseteq N$；现规定：对于 $\forall n_1\in N_1$，$t:n_1\mapsto h(n_1)\in N$，则 t 是 N_1 到 N 的同态，并且 $gt=h$，即图 19.20 是交换图：故 g 是 f 的核.

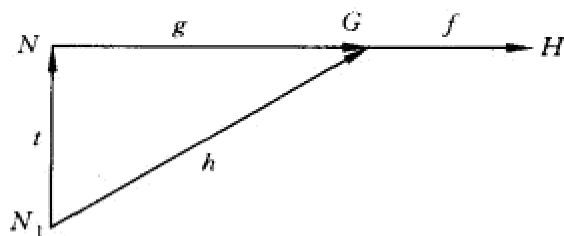


图 19.20

(2) 同样可证在 Ab, Ring, R-mod 等范畴中，态射 $f\in$ hom(A,B)的核就是同态 f 的(同态)核到 A 的一个单同态.

注 19.8.3 关于核定义的说明　同态核是一个对象，但态射的核却是一个单态射，但是这二者实际上是一致的，因为当 $g\in$ hom(C,A)给定后，对象 C 就确定了；反过来，若给定对象 C,A 后，hom(C,A)的态射可能不唯一，取其中的哪一个作为态射的核不能确定，不如直接采用态射本身来表示核.

定理 19.8.4 设 $f\in$ hom(A,B)，若 f 有核 $g\in$ hom(C,A)，则 f 的核(从同构的观点看)是唯一的，记为 ker$f$.

由对偶原则可以得到核的对偶概念.

定义 19.8.5 设范畴 $\mathscr{C}$ 有零对象，因而有零态射，设 $f\in$ hom(B,A)，则态射 $g\in$ hom(A,C)称为 f 的**上核**(co-kernel)，如果它满足以下条件：

(1) g 是满态射；

(2) $gf=0_{BC}$；

(3) 对于 $\forall h\in$ hom(A,D)，若 $hf=0_{BD}$，则必有 $t\in$ hom(C,D)，

使 $h=tg$,即其图是交换图 19.21.

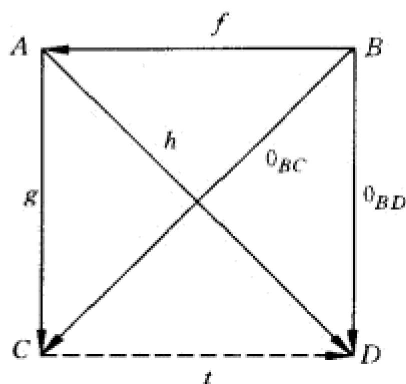


图 19.21

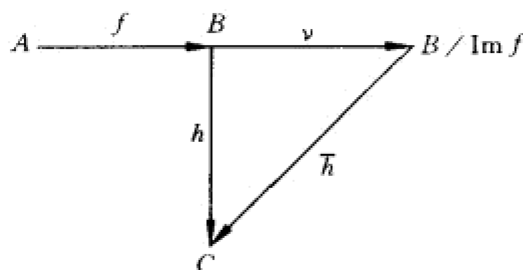


图 19.22

定理 19.8.6 设 $f\in\hom(B,A)$,若 f 有上核,$g\in\hom(A,C)$,则 f 的上核(从同构的观点看)是唯一的,记为 $\mathrm{cok}f$.

例 19.8.7 在 R-mod 中,$f\in\hom(A,B)$,f 的同态像 $\mathrm{Im}f=f(A)$是 B 的子模,则 $B/\mathrm{Im}f$ 是 R-模.设 ν 是 B 到 $B/\mathrm{Im}f$ 的自然同态,则可断言,$\nu=\mathrm{cok}f$,这是因为:

(1) ν 是满同态,因而是满态射;

(2) 对于 $\forall a\in A$,$\nu f(a)=0$,所以 $\nu f=0$;

(3) 若 $h\in\hom(B,C)$且 $hf=0$,即 $h(\mathrm{Im}f)=0$,

所以有导出同态 $\bar{h}:B/\mathrm{Im}f\to C$ 使 $h=\bar{h}\nu$,这表示图 19.22 是可交换的,所以 $\nu=\mathrm{cok}f$.

19.9 拉回与推出

定义 19.9.1 在范畴 $\mathscr{C}$ 中,态射 $f_1=\hom(A_1,X)$及 $f_2=\hom(A_2,X)$的**拉回**(pullback)是指一个对象 Y 和两个态射 g_1,g_2 所成的三元组 $\langle Y;g_1,g_2\rangle$,满足下述条件:对于 $g_1\in\hom(Y,A_1)$及$g_2\in\hom(Y,A_2)$,能使 $f_1g_1=f_2g_2$,并且对任意的

对象 Z 及任意的 $h_1 \in \hom(Z,A_1)$ 及 $h_2 \in \hom(Z,A_2)$，当 $f_1h_1 = f_2h_2$ 时，存在唯一的 $t \in \hom(Z,Y)$ 使 $h_1 = g_1t$，$h_2 = g_2t$，即有交换图 19.23.

定理 19.9.2 在范畴 $\mathscr{C}$ 中，二态射 $\{f_1, f_2\}$ 的拉回如果存在，则（从同构的观点看）它是唯一的.

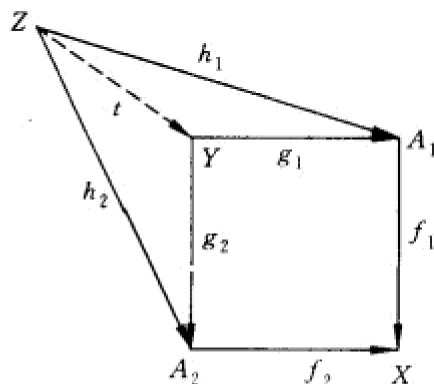


图 19.23

例 19.9.3 设 $f_1 \in \hom(A_1, X)$ 及 $f_2 \in \hom(A_2, X)$ 是模范畴 R-mod 的两个态射，则可证明 $\{f_1, f_2\}$ 的拉回是 $\langle Y; g_1, g_2 \rangle$，其中 $Y = \{(a_1, a_2) \mid a_i \in A_i$ 且 $f_1(a_1) = f_2(a_2)\}$，$g_1 : (a_1, a_2) \mapsto a_1$，$g_2 : (a_1, a_2) \mapsto a_2$.

两个态射的拉回能够保持单态射性质.

定理 19.9.4 设 $\{f_1, f_2\}$ 的拉回是 $\langle Y; g_1, g_2 \rangle$，若 f_1（或 f_2）是单态射，则（在交换图中）与它平行的态射 g_2（或 g_1）也是单态射.

与拉回对偶的概念是推出，可用对偶原则给出它的定义和性质如下.

定义 19.9.5 在范畴 $\mathscr{C}$ 中，态射 $f_1 \in \hom(X, A_1)$ 及 $f_2 \in \hom(X, A_2)$ 的**推出**（pushout）是指一个对象 Y 和两个态射 g_1, g_2 所成的三元组 $\langle Y; g_1, g_2 \rangle$ 满足下述条件：对于 $g_1 \in \hom(A_1, Y)$，$g_2 \in \hom(A_2, Y)$，它们能使 $g_1f_1 = g_2f_2$，并且对任意的对象 Z 及任意的 $h_1 \in \hom(A_1, Z)$ 及 $h_2 \in \hom(A_2, Z)$，当 $h_1f_1 = h_2f_2$ 时，存在唯一的 $t \in \hom(Y, Z)$ 使 $h_1 = tg_1$，$h_2 = tg_2$，即有交换图 19.24.

定理 19.9.6 在范畴 $\mathscr{C}$ 中，$\{f_1, f_2\}$ 的推出如果存在，则（从同构的观点看）它是唯一的.

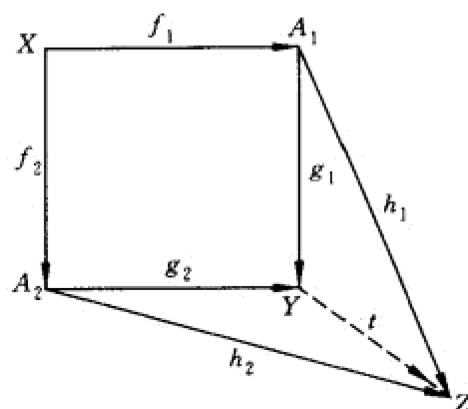


图　19.24

例 19.9.7　设 $f_1 \in \hom(X, A_1)$ 及 $f_2 \in \hom(X, A_2)$ 是模范畴 R-mod 的两个态射，则它们的推出是 $\langle Y; g_1, g_2 \rangle$，其中 $Y = (A_1 \oplus A_2)/W$，这里的 $W = \{(f_1(x), -f_2(x)) \mid x \in X\}$，

$g_1: a_1 \mapsto \overline{(a_1, 0)}$，$g_2: a_2 \mapsto \overline{(0, a_2)}$. $\overline{(a_1, 0)}$，$\overline{(0, a_2)}$

分别是商模 $(A_1 \oplus A_2)/\overline{W}$ 的元，即利用 W 分类时元 $(a_1, 0)$ 及 $(0, a_2)$ 所在的类.

证明可通过图 19.25 看出.

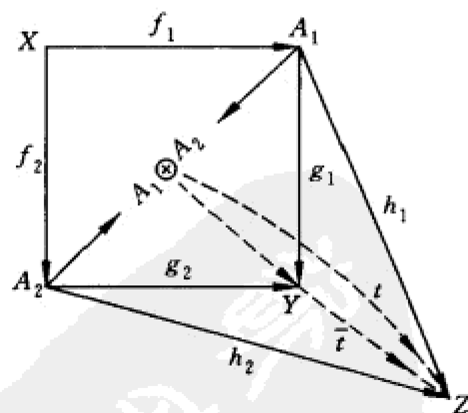


图　19.25

两个态射的推出能够保持双态射性质.

定理 19.9.8 设$\{f_1, f_2\}$的推出是$\langle Y; g_1, g_2\rangle$，若 f_1（或 f_2）是满态射，则（在交换图中）与它平行的态射 g_2（或 g_1）也是满态射.

19.10 hom 函子与可表示函子

本节先介绍三种 hom 函子，它们分别是范畴 $\mathscr{C}$，$\mathscr{C}^\circ$及 $\mathscr{C}^\circ \times \mathscr{C}$ 到集范畴 Set 的函子，在考察了它们的性质后再研究已知的函子由 hom 函子表示的问题.

先看范畴 $\mathscr{C}^\circ \times \mathscr{C}$，它的对象类是由一切偶对$(A, B)$ $(A, B \in \mathrm{ob}\mathscr{C})$构成的，它的从$(A, B)$到$(A', B')$的态射是偶对$(f, g)$，其中 $f: A \to A'$，$g: B \to B'$；又若(f', g')是 $\mathscr{C}^\circ \times \mathscr{C}$ 的从(A', B')到(A'', B'')的一个态射，则 $f': A' \to A''$，$B' \to B''$，因而$(f', g')(f, g) = (f'f, g'g)$. 此外 $1_{(A,B)} = (1_A, 1_B)$.

定义 19.10.1 由 $\mathscr{C}^\circ \times \mathscr{C}$ 到 Set 的 hom 函子，这种函子的对象函数是将它的每个对象(A, B)映射到集 $\hom(A, B)$ $(\in \mathrm{ob}$ Set)，而它的态射函数则是将$(f, g): (A, B) \to (A', B')$射入到 $\hom(A, B)$到 $\hom(A', B')$里的映射的函数，其对应法则是：

$$\hom(f, g): k \mapsto gkf,$$

其中 $f: A' \to A$，$g: B \to B'$，$k: A \to B$，因而此法则是有意义的，且 $gkf: A' \to B'$，这样的规定确能构成一个函子，称为**由 $\mathscr{C}^\circ \times \mathscr{C}$ 到 Set 的 hom 函子**.

定义 19.10.2 固定 $\mathscr{C}$ 的一个对象 A 并按下列法则定义的函子 $\hom(A, -)$[*] 称为**由 $\mathscr{C}$ 中对象 A 确定的（共变）hom 函子**：

(1) 对象函数

---

[*] 表达式 $\hom(A, -)$表示一种特殊的函子（符号）.

$\hom(A,-)B^{*}=\hom(A,B)$;

(2) 态射函数

对于 $g:B\to B'$,$\hom(A,-)(g)$是 $\hom(A,B)$到 $\hom(A,B')$内的映射,其对应法则为

$$\hom(A,g):k\mapsto gk.$$

定义 19.10.3 固定$\mathscr{C}$的一个对象 B 并按下列法则定义的函子 $\hom(-,B)$称为**由$\mathscr{C}$中对象 B 确定的(反变)hom 函子.**

(1) 对象函数

$$\hom(-,B)A=\hom(A,B).$$

(2) 态射函数

对于 $f:A'\to A$,$\hom(-,B)(f)$是 $\hom(A,B)$到 $\hom(A',B)$内的映射,其对应法则是

$$\hom(f,B):k\mapsto kf.$$

比较以上三种函子有以下联系.

定理 19.10.4 设 $f:A'\to A,g:B\to B',k:A\to B$,

则因 $\hom(f,B')\hom(A,g)(k)=(gk)f$,

$\hom(A',g)\hom(f,B)(k)=g(kf)$,

$\hom(f,g)(k)=(gk)f=g(kf)$.

所以三者相等,并得到交换图 19.26.由它可找到函子间的两个自然变换,这对于用 hom 函子表示一个给定的函子极为有用.

定理 19.10.5 (1) 取定 $g:B\to B'$后,映射 $A\mapsto\hom(A,g)\in\hom_{Set}(\hom(A,B),\hom(A,B'))$是反变函子 $\hom(-,B)$到反变函子 $\hom(-,B')$内的自然变换.

(2) 取定 $f:A'\to A$ 后,映射 $B\mapsto\hom(f,B)\in\hom_{Set}(\hom(A',B),\hom(A,B))$是函子 $\hom(A,-)$到函子 $\hom(A',-)$内的自然变换。

---

* 表达式 $\hom(A,-)B$ 表示函子 $\hom(A,-)$作用于对象 B.

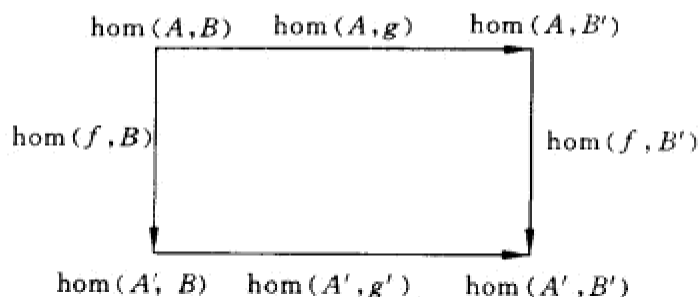


图 19.26

要将一个函子用一个 hom 函子“表示”,需要以下定理.

定理 19.10.6 Yoneda Lemma 定理 设 F 是由 $\mathscr{C}$ 到 Set 的函子,A 是 $\mathscr{C}$ 的一个对象,a 是集 FA 的一个元. 对于 $\forall B \in \mathrm{ob}\mathscr{C}$,设 a_B 是 $\hom_{\mathscr{C}}(A,B)$到 FB 内的、使 $k \mapsto F(k)(a)$的映射,则 $B \mapsto a_B$ 是 $\hom_{\mathscr{C}}(A,-)$到 F 内的一个自然变换 $\eta(a)$. 此外,$a \mapsto \eta(a)$是集 FA 到 $\hom_{\mathscr{C}}(A,-)$到 F 的自然变换类上的一个双射,$a \mapsto \eta(a)$的逆(映射)是映射 $\eta \mapsto \eta_A(1_A)$(这里的 $\eta_A(1_A) \in FA$).

定义 19.10.7 (1) 设 F 是由 $\mathscr{C}$ 到 Set 的一个函子,若对于某个 $A \in \mathrm{ob}\mathscr{C}$ 存在 F 与函子 $\hom(A,-)$间的一个自然同构,则称函子 F 是**可表示的**(representable functor).

(2) 设 F 是一个可表示函子,η 是 F 与函子 $\hom(A,-)$间存在的自然同构,若 Yoneda 预备定理中用以决定 η 的对象及元分别是 A 及 $a(=\eta_A(1_A) \in F_a)$,则偶对(A,a)称为**可表示函子的表示**(representative of the representable functor).

19.11 加法范畴与 Abel 范畴

本节介绍两个重要的范畴,它们在模论及同调代数中经常使用.

定义 19.11.1 设 $\mathscr{C}$ 是范畴,若能满足以下 4 个条件,则称为

加法范畴(additive category):

(1) $\mathscr{C}$ 有一个零对象(定义 19.2.13).

(2) 对于 $\mathscr{C}$ 中的每一个对象偶(A,B),在集 $\hom_{\mathscr{C}}(A,B)$上定义一个二元复合运算"+"使得$\langle \hom_{\mathscr{C}}(A,B),+,O_{AB}\rangle$是交换群.

(3) 若 $A,B,C\in \mathrm{ob}\mathscr{C}$, $f,f_1,f_2\in \hom_{\mathscr{C}}(A,B)$及 $g,g_1,g_2\in \hom_{\mathscr{C}}(B,C)$,则

$$(g_1+g_2)f = g_1f+g_2f,$$
$$g(f_1+f_2) = gf_1+gf_2.$$

(4) $\mathscr{C}$ 是有上积的范畴,即 $\mathscr{C}$ 的对象的任一有限集均存在上积.

例 19.11.2 群范畴 Grp 是加法范畴,因为它有零对象$\{0\}$(即仅含一个加法单元的群).当群的复合运算记成乘法时,这个零对象是$\{1\}$(即仅含一个乘法单元的群),它既是始对象又是终对象(定义 19.2.13),所以满足(1);此外它满足(2)(3)也是显然的,因为范畴上的态射满足这两个条件;据定理 19.7.8 可知:群范畴 Grp 的对象的任一标号集的上积是存在的,因此满足(4).故 Grp 是加法范畴.

例 19.11.3 交换群范畴 Ab,环范畴 Ring,左、右模范畴 R-mod 及 mod-R 都是加法范畴.

例 19.11.4 集范畴 Set 不是加法范畴,因为它没有零对象(例 19.2.14(1)).

注 19.11.5 关于定义的说明

(1) 定义条件(2)表示在每个 $\hom_{\mathscr{C}}(A,B)$上给定了一个群结构,其零元是 $0_{AB}=0_{OB}\cdot 0_{AO}$,这里 0_{AO}是 $\hom_{\mathscr{C}}(A,0)$的唯一元,0_{OB}是 $\hom_{\mathscr{C}}(0,B)$的唯一元.

(2) 定义条件(3)说明:当用范畴定义时,乘积 fg 是双可加的(bi-additive),因而对于每个 A 都可决定一个环结构$\langle \hom_{\mathscr{C}}(A,A);+,\cdot;0,1=1_A\rangle$.

(3) 定义条件(4)可用以下两个条件之一代替，因为这三个条件是等价的：

(4) $\mathscr{C}$是具有积的范畴.

(5) 对于对象的任一有限集$\{A_1,\cdots,A_n\}$存在对象 A 及态射 $p_j:A\to A_j$，$i_j:A_j\to A(1\leqslant j\leqslant n)$，使

$$p_k i_j=\begin{cases}1_{A_j}, 若\ j=k,\\0, 若\ j\neq k,\end{cases}$$

$$\sum i_j p_j=1_A.$$

由加法范畴定义的对偶性可得以下定理.

定理 19.11.6 若 $\mathscr{C}$ 是加法范畴，则其对偶范畴(定义 19.2.6)$\mathscr{C}^{\circ}$也是加法范畴.

下面进一步讨论 Abel 范畴.

定义 19.11.7 设$\mathscr{C}$是加法范畴，若还满足以下三个条件，则称为 **Abel 范畴**(Abel category)：

(1) $\mathscr{C}$中的每个态射都有一个核及一个上核.

(2) 每个单(满)态射都是它的上核(核)的核(上核).

(3) 每个态射都能分解成一个满态射 e 与一个单态射 m 的乘积：$f=m\cdot e$.

例 19.11.8 (1) 交换群范畴 Ab 是 Abel 范畴：首先它是加法范畴(例 19.11.3)，而且它的每个态射都有核与上核.

(2) 范畴 R-mod 及 mod-R 都是 Abel 范畴.

(3) 可以证明：以所有自由交换群(例 19.11.3)为对象、以群同态为态射构成的自由交换群范畴 FAG 是加法范畴，但却不是 Abel 范畴，因为它的态射不一定有上核.

19.12 通用结构

各种代数系统中经常存在一些"通用"结构，它们所具有的代

数性质可以通过态射“传输”到同类结构中去. 例如，自然数 1 是所有单元半群（以及所有群）的“通用元”，这是因为在加法单元半群 $\boldsymbol{N}$ 与任一单元半群 M 间存在着（单元半群）同态：

$$f:\boldsymbol{N}\to M, 1\mapsto a(a\in M),$$

因此二者有相同的代数性质. 这也可以说：态射 f 将 $\boldsymbol{N}$ 的“通用”性质“传输”给 M 了；对于群 G 也有同样的结论. 此外，各种商结构（包括商集、商群、商环等）、分式域、多项式环等的态射间都存在着某些通用性质，由于它们的讨论牵涉到某类代数结构及其间的态射，所以可利用范畴和函子对它们作精确的描述.

定义 19.12.1 设 $\mathscr{C},\mathscr{D}$ 是两个范畴，F 是由 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，B 是 $\mathscr{D}$ 的对象，由 B 到函子 F 的**通用结构**(universal construction)是一个偶对 (U,u)，其中 U 是 $\mathscr{C}$ 的对象而 u 是由 B 到 FU 的态射，它能使：若 g 是由 B 到 FA 的任一态射，则存在唯一的由 U 到 $\mathscr{C}$ 中的 A 的态射 $\tilde{g}$，使

$$g=F(\tilde{g})\cdot u.$$

即图 19.27 是一个可交换图.

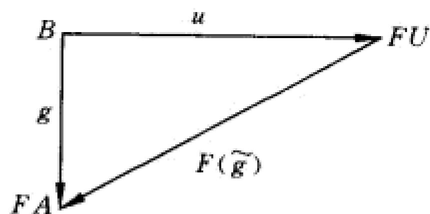


图 19.27

U 称为 **B 的一个通用 $\mathscr{C}$-对象**(universal $\mathscr{C}$-object for B)，而态射 u 称为**对应的通用映射**(corresponding universal map).

例 19.12.2 (1) 设 $X=\{x_1,x_2,\cdots,x_r\}$，作序列集 $FS^{(r)}=\{(x_{i_1},x_{i_2},\cdots,x_{i_m})\mid x_{i_j}\in X, m=1,2,3,\cdots\}$，并规定其乘法为“连接”，即

$(x_{i_1},x_{i_2},\cdots,x_{i_m})(x_{j_1},x_{j_2},\cdots,x_{j_n})=(x_{i_1},\cdots,x_{i_m},x_{j_1},\cdots,x_{j_n})$，然后加入单元 1，即可得一单元半群 $FM^{(r)}$，称为由 r 个元 x_i 生成的自由单元半群.

在此基础上作集 $X\cup X'$，其中 X 为集 $\{x_1,x_2,\cdots,x_r\}$，x'为另

一集$\{x_1',x_2',\cdots,x_r'\}$，它们不相交而且在$X$与$X'$间有1-1对应：$x_i \leftrightarrow x_i'$，仿上作出由$X\cup X'$生成的自由单元半群$FM^{(2r)}$. 现设$G$是群而且$a_1,a_2,\cdots,a_r$是$G$的元素序列，则可作唯一的同态$\eta: F^{(2r)} \to G, x_i \mapsto a_i, x_i' \mapsto a_i^{-1}, 1\leqslant i\leqslant r$. 由同态基本定理可得$FM^{(2r)}$上的同余关系$E_\eta: aE_\eta b \Leftrightarrow \eta(a)=\eta(b)$，从而得同余类$[x_i](1\leqslant i\leqslant r)$生成的自由群$FG^{(r)}=FM^{(2r)}/\equiv$. 它有如下的通用性质.

作X到$FG^{(r)}$内的映射$i: x\mapsto \bar{x}$，则对于任意群G及X到G内的映射g必有唯一的同态$\tilde{g}: FG^{(r)}\to G$使$g=\tilde{g}i$，即图19.28是可交换图.

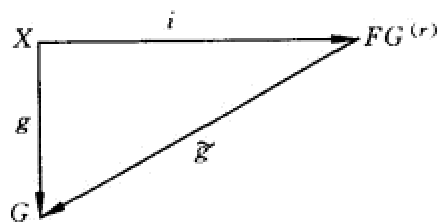


图 19.28

用范畴与函子表示这个通用结构. 考虑范畴Grp及Set并使F为Grp到Set的忘却函子，它将一个群映射到它的基集，而将群同态映射映入对应的集映射. 现给定一集X，被X确定的自由群是一个偶对(U,u)，这里的U是一个群，而u则是X到U内的映射，它对于任意的群G及X到G内的映射g都有唯一的由U到G内的同态$\bar{g}$，使$\bar{g}u=g$对于集映射成立. 所以，X到函子F的通用结构是(U,u)，其中U是X的通用Grp对象，而u则是对应的通用映射.

(2) 域上的李代数(定义17.4.1)L是具有双线性积$[xy]$而能使$[xx]=0$及$[[xy]z]+[[yz]x]+[[zx]y]=0$的向量空间. 若$A$是一个结合代数(17.1节)，由$A$可定义李代数$A^-$，这只需将**李积**(或称加法交换子)$[xy]=xy-yx$(这里$xy$是$A$中已有的结合乘法)作为它的复合运算. 显然，若$A$及$B$都是结合代数而且$f$是$A$到$B$内的同态，则$f$也是$A^-$到$B^-$中的李代数同态.

若L是李代数，L的**通用包络代数**(universal enveloping algebra)是一个偶对$(U(L),u)$，其中$U(L)$是结合代数而u是L

到李代数$U(L)^-$内的同态，它使得：若g是L到由结合代数A得到的李代数A^-中的任一同态，则存在唯一的由结合代数$U(L)^-$到A^-内的同态$\tilde{g}$，使得

$$g=\tilde{g}u.$$

图 19.29 是李代数同态的交换图.

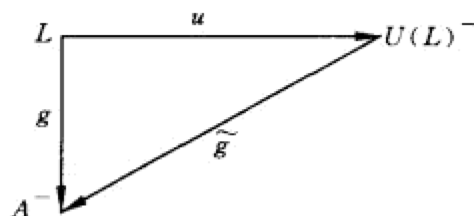


图 19.29

取给定域上的结合代数范畴 Alg 及李代数范畴 Lie，定义由 Alg 到 Lie 的函子F如下：对于结合代数A，规定$FA=A^-$；而对于结合代数中的态射$f:A\to B$，则使相应的李代数中的$F(f)=f:A^-\to B^-$与之相应. 对于给定的李代数L，通用的包络是一个偶对$(U(L),u)$，其中$U(L)$是结合代数，而u是L到$U(L)^-$内的一个李代数同态，它使得如果g是L到李代数A^-（A是结合的）内的任一同态，则必然存在唯一的$U(L)$到A^-中的同态$\tilde{g}$，使得$\tilde{g}u=g$.

(3) 交换整环的分式域：令 Dom 表示范畴 Ring 的子范畴，它的对象是交换整环（即无零因子的交换环），它的态射是单态射，它显然是 Ring 的一个子范畴，而且它还有完满子范畴 Field（其对象为域，态射为单态射）. 若D是交换整环，则D有分式域F，F的一个重要性质是：有由D到F的单态射$u:a\mapsto a/1$，而当g是D到域F'内的任一单同态时，存在唯一的F到F'内的单态射$\tilde{g}$使得$g=\tilde{g}u$. 因此，可将D与分式$d/1$的集等同看待并且能取u为单映射. 这样就将$D(\subset F)$的任一单态射唯一地扩张成F到F'内的单态射了. 这个结果可如下纳入通用结构的定义：作子范畴 Field 到范畴 Dom 的单射函子（例 19.4.3(1)），若D是交换整环，因而是 Dom 的一个对象. 故D的在 Field 中的通用对象是D的分式域F，而通用映射u则为将D射入F的单射，偶对(F,u)即为从D到

单射函子的通用结构.

求通用结构的方法可能有多种多样,但从同构的观点看它们是唯一的.

定理 19.12.3 设(U,u)及(U',u')都是从对象 B 到函子 F 的通用结构,则必存在唯一的同构 $h:U\to U'$使 $u'=F(h)u$.

此外,还可给出通用结构的对偶定义如下.

定义 19.12.4 设$\mathscr{C}$及$\mathscr{D}$是两个范畴,G是由$\mathscr{D}$到$\mathscr{C}$的函子,$A\in \mathrm{ob}\mathscr{C}$,则由函子 G 到 A 的通用结构是一个偶对(V,v),其中 $V\in \mathrm{ob}\mathscr{D}$,而 $v\in \mathrm{hom}_{\mathscr{C}}(GV,A)$,它满足:若 $B\in \mathrm{ob}\mathscr{D}$ 及 $g\in \mathrm{hom}_{\mathscr{C}}(GB,A)$,则存在唯一的 $\tilde{g}:B\to V$ 使 $vG(\tilde{g})=g$.

19.13 伴随函子

本节就范畴$\mathscr{D}$的每个对象 B 都存在由 B 到函子 F 的通用结构(U,u)的情况下讨论伴随函子的问题,这种函子对于将代数系统的构造描述成适当范畴上的函子有重要的作用.

定理 19.13.1 设 F 是由$\mathscr{C}$到$\mathscr{D}$的函子,它对于每个 $B\in \mathrm{ob}\mathscr{D}$总存在一个 B 到 F 的通用结构. 现对每个 B 选择称之为(GB,u_B)的通用结构. (1)若在$\mathscr{D}$中 $h:B\to B'$,现规定 $G(h):GB\to GB'$是 $\mathrm{hom}_{\mathscr{C}}(GB,GB')$中能使 $F(G(h))u_B=u_{B'}h$ 的唯一的元素,则 G 必为$\mathscr{D}$到$\mathscr{C}$的一个函子. (2)若 $A\in \mathrm{ob}\mathscr{C}$,总存在唯一的 $v_A:GFA\to A$ 使 $F(v_A)u_{FA}=1_{FA}$,则(FA,v_A)是由 G 到 A 的通用结构. (3)若 $\eta_{B,A}$是 $\mathrm{hom}_{\mathscr{C}}(GB,A)$到 $\mathrm{hom}_{\mathscr{D}}(B,FA)$内的映射 $f\mapsto F(f)u_B$,则对于固定的 B,$A\mapsto\eta_{B,A}$是由 $\mathrm{hom}_{\mathscr{C}}(GB,-)$到 $\mathrm{hom}_{\mathscr{D}}(B,F-)$的自然同构,而且对于固定的 A,$B\mapsto\eta_{B,A}$是 $\mathrm{hom}_{\mathscr{C}}(G-,A)$到 $\mathrm{hom}_{\mathscr{D}}(-,FA)$的自然同构.

由此定理,D. M. Kan 引进了如下的伴随函子概念.

定义 19.13.2 设 F 是由$\mathscr{C}$到$\mathscr{D}$的函子,G是由$\mathscr{D}$到$\mathscr{C}$的函

子，若对于每个偶对(B,A)，$(A\in \mathrm{ob}\mathscr{C}, B\in \mathrm{ob}\mathscr{D})$存在一个双射$\eta_{B,A}$，

$$\eta_{B,A}:\mathscr{C}(GB,A)\cong\mathscr{D}(B,FA),$$

且对于每个B，$A\mapsto\eta_{B,A}$是$\hom_{\mathscr{C}}(GB,-)$到$\hom_{\mathscr{D}}(B,F-)$的自然同构，对于每个A，$B\mapsto\eta_{B,A}$是$\hom(G-,A)$到$\hom_{\mathscr{D}}(-,FA)$的自然同构，则称F为G的**右伴随函子**(right adjoint functor)，记作$G\dashv F$. 而G称为F的**左伴随函子**(left adjoint functor). 映射$\eta:(B,A)\mapsto\eta_{B,A}$称为$G$到$F$的**伴随**(adjugant)；三元组$\langle F,G,\eta\rangle$称为**接合**(adjunction).

例 19.13.3 定理 19.13.1 中，由B到F的通用结构(U,u)决定的$\langle F,G,\eta\rangle$是一个接合；反之，当接合给定后，通用结构(U,u)也可以被决定. 而且从同构的观点看它们都是唯一的，因为有以下定理.

定理 19.13.4 由$\mathscr{C}$到$\mathscr{D}$的函子F的任意两个左伴随函子G与G'都是自然同构的.

20 泛代数

本章继续研究各种代数结构，着眼点放在代数结构的运算系统，这与 19 章把对象、态射、函子、自然变换等作为研究重点有所不同.

泛代数作为代数的比较研究起源于哲学家、数学家 A. N. Whitehead，他于 1898 年发表了著作“A Treatise on Universal Algebra With Applications”(《论泛代数及其应用》)，提出了对 Hamilton 四元数系，Grassmann 扩张演算(calculus of extensions)及布尔符号逻辑进行比较研究的建议，由于当时条件尚不成熟未能得到充分的发展，直到 20 世纪 30 年代后经过 G. Birkhoff，Tarski，Jossen 等人的努力才得到一系列重要的成果；20 世纪 60 年代以后 Grätzer，Cohn，S. Burris 及 H. P. Sankappanavar 先后出版了泛代数方面的专著才得到了推广和运用，目前它已广泛应用于数理逻辑、模型论、证明论、语言代数、计算语言学等领域之中.

20.1 Ω 代数

从前面各章中可以发现，在不同的代数结构中有很多平行的性质，最明显的是同态基本定理，它在群、环、模、代数中都成立，而且内容“基本相似”，理应建立一个统一的理论.

定义 20.1.1 设 $n\in \mathbf{N}^{+}$，A 是集，则 A^n 到 A 的映射 $\omega: A^n\to A$，

$$(a_1,a_2,\cdots,a_n)\mapsto a=\omega(a_1,a_2,\cdots,a_n),\ (a_i\in A),$$

称为集 A 上的 **n 元运算**(n-ary operation)，元素 $a=\omega(a_1,a_2,\cdots,$

a_n)称为元素 $a_1, a_2, \cdots, a_n$ 的 **n 元积**(n-ary product),通常简写为 $\omega a_1 a_2 \cdots a_n$.

当 $n=0$ 时,规定**零元积** $\omega(0)$ 为 A 的某一特异元(distinguished element)(例如环 R 的零元积 $\omega(0)=0_R$,即环 R 的零元).

非负整数 n 称为运算的**元数**(arity).

集 A 上的 n 元运算 $\omega(n)$,对于非负整数 n,它的所有 n 元运算的全体用 $\Omega(n)$ 表示,则 A 上的所有"运算"构成的**运算系** Ω 可表示成 $\Omega=\bigcup_n \Omega(n)$.

例 20.1.2 群 G 的乘法"·"是二元运算,求元素的逆的运算"$^{-1}$"是它的一元运算,此外群 G 的单元 1 是唯一存在的特异元,因此求 G 的 1 是它的零元运算.因而 G 的运算系 $\Omega=\{\cdot, ^{-1}, 1\}$.

定义 20.1.3 非空集 A 连同 n 元运算系 Ω 所构成的代数结构称为**泛代数**(universal algebra/Ω algebra)或 **Ω 代数**.该运算系一般是有限的,也可以是无限的(如无限域上的向量空间有一个二元运算、即加法和无限多个一元运算、即它与基本域的元的算子乘法).

例 20.1.4 (1) 单元半群 M 是 Ω 代数,其基集是 M,运算系是 $\Omega=\{\cdot, 1\}$,这里"·"是二元运算而 1 是零元运算.它们满足下列各等式:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$

$$a \cdot 1 = 1 \cdot a = a \qquad (1 \text{ 是单元}).$$

(2) 群是 Ω 代数,其基集为 G,它的运算系是 $\Omega=\{\cdot, ^{-1}, 1\}$,其中"·"是二元运算,"1"是零元运算,"$^{-1}$"是求元 a 的逆元素的运算,是一元运算.

(3) 环是 Ω 代数,其运算系 $\Omega=\{+, \cdot, 0, 1, -\}$,其中"+ ·"分别是求和与求积,均为二元运算;"0,1"为求环的零元与单元,均为零元运算;"−"是取元 a 的逆元 $-a$.它们所满足的恒等式容易

从环的公理得到.

(4) 算子群(或 Λ 群)是 Ω 代数,此时运算系 $\Omega=\Lambda\cup\{\cdot,^{-1},1\}$,其中 $\cdot,^{-1},1$ 与群相同,Λ 是异于 $\cdot,^{-1},1$ 的一元运算符号,它们所满足的恒等式除包括群的所有恒等式外还有 $\lambda(a\cdot b)=(\lambda a)\cdot(\lambda b)$.

(5) 格是 Ω 代数,它的运算系 $\Omega=\{\vee,\wedge\}$,其中 $\vee,\wedge$ 分别是"取并"及"取交",它们都是二元运算.

(6) 域不是 Ω 代数,因为它的除法(乘法的逆运算)不是对整个域都能施行的. 此外模论也很难用上 Ω 代数的结果,因为作为媒介的算子集并不能反映环的结构.

20.2 子代数与积

定义 20.2.1 设 A 是任一 Ω 代数,B 是它的非空子集,若对于任意 $\omega\in\Omega(n)$ 及 $(b_1,b_2,\cdots,b_n)$,$b_i\in B$,$\omega b_1 b_2\cdots b_n\in B$(特别地,当 $n=0$ 时,特异元 $\omega_A\in B$),则称 B 为 A 的**子代数**(subalgebra).

例 20.2.2 (1) 若 A 是群,它的子集 B 是一个子群当且仅当对于 $\forall b,c\in B$ 都有 $b\cdot c,1$ 及 $b^{-1}\in B$.

(2) 设 B 是 A 的子代数,C 是 B 的子代数,则 C 是 A 的子代数.

(3) 设 $\{B_\alpha|\alpha\in I\}$ 是子代数 B_α 的集,则它们的交 $\bigcap_{\alpha\in I}B_\alpha$ 是一个子代数或空集.

(4) 将空集 $\varnothing$ 加入 Ω 代数 A 的所有子代数 $B_\alpha(\alpha\in I)$ 的集 $\{B_\alpha\}$ 中,并按包含关系将其偏序化,则 $\{B_\alpha\}$ 作成一个完全格,交集 $\bigcap_{\alpha\in I}B_\alpha$ 作成一个子代数,而且它也是这个格的最小上界(sup).

下面要问 $\{B_\alpha\}$ 的并集 $\bigcup_\alpha B_\alpha$ 是否是子代数? 是否是最小上界? 一般来说,它可能不是子代数,也未必是 sup. 我们仅就一种

情况回答这个问题,即在$\{B_\alpha\}$被包含关系定向时它是一个子代数且是B_α的sup,为此先给出定向的概念.

定义 20.2.3 设$\{B_\alpha\}$是子代数B_α的集,如果对于$\forall B_\beta, B_\gamma \in \{B_\alpha\}$,存在一个$B_\delta$使得$B_\delta \supset B_\beta$及$B_\delta \supset B_\gamma$,则称$\{B_\alpha\}$**被包含关系定向**(directed by inclusion). 例如每个全序集或链是被包含关系定向的.

定理 20.2.4 设$\{B_\alpha\}$是子代数定向集,则$\bigcup B_\alpha$是子代数且是$\{B_\alpha\}$的sup.

下面再介绍两种类型的子代数.

例 20.2.5 (1) 由集X生成的子代数$[X]$. 设X是Ω代数A的非空子集,$\{B_\alpha\}$是A中包含X的一切子代数的集,作$\bigcap B_\alpha$,则$\bigcap B_\alpha=[X]$,它可以如下递归地作出:

令$X_0=X\bigcup U$,其中U是特异元ω_A的集,而$\omega\in\Omega(0)$;对于$k\geqslant 0$令$X_{k+1}=X_k\bigcup\{Y|Y=\omega x_1\cdots x_n, x_i\in X_k, \omega\in\Omega(n), n\geqslant 1\}$.

显然$X_0\subset X_1\subset X_2\subset\cdots$,而且$[X]=\bigcup X_k$.

(2) Ω代数的标号族$\{A_\alpha|\alpha\in I\}$的积. 设$\{A_\alpha|\alpha\in I\}$是Ω代数族,其标号集$I=\{1,2,\cdots,r\}$,这些A_α可以是若干个相同甚至完全相同. 作乘积$\prod_I A_\alpha = A_1\times A_2\times\cdots\times A_r$,则可以证明它是$\Omega$代数,称为$\Omega$代数的标号族$\{A_\alpha\}$的积,此代数的每个元是一个$r$元组$(a_1,a_2,\cdots,a_r)$,其运算规律如下:

1) 若ω是零元运算,则$A_1\times A_2\times\cdots\times A_r$的相应元为$(\omega_{A_1},\omega_{A_2},\cdots,\omega_{A_r})$,这里$\omega_{A_i}$是$A_i$中的特异元;

2) 若$n\geqslant 1$且$a^{(i)}=(a_1^{(i)},a_2^{(i)},\cdots,a_r^{(i)})(1\leqslant i\leqslant n)$,则$\omega a^{(1)}a^{(2)}\cdots a^{(n)}$是$A_1\times A_2\times\cdots\times A_r$的元,由于

$$a^{(1)} = (a_1^{(1)},a_2^{(1)},\cdots,a_i^{(1)},\cdots,a_r^{(1)}),$$
$$a^{(2)} = (a_1^{(2)},a_2^{(2)},\cdots,a_i^{(2)},\cdots,a_r^{(2)}),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

…………………………………

$$a^{(n)} = (a_1^{(n)}, a_2^{(n)}, \cdots, a_i^{(n)}, \cdots, a_r^{(n)}),$$

所以 $\omega a^{(1)} a^{(2)} \cdots a^{(n)}$ 的第 i 个分量是

$$\omega a_i^{(1)} a_i^{(2)} \cdots a_i^{(n)}.$$

20.3 同态与同余

同所有代数结构一样，本节将讨论 Ω 代数的同态、同余以及利用同余（关系）构造商代数的方法和有关定理，最后举例说明这些定理的重要性和高度概括性.

定义 20.3.1 设 Ω 代数 A 与 A' 的运算系 Ω 与 Ω' 之间存在 1-1 对应，在此对应下，任意运算 $\omega \in \Omega$ 和与之相应的运算 $\omega' \in \Omega'$ 是有相同元数的 n 元运算，则称 A 与 A' 是**同型代数**(algebras of same type).

两个同型代数可认为有相同的运算系.

定义 20.3.2 设 A 及 B 是两个 Ω 代数，如果存在由 A 到 B 的映射 f 能使每个 $\omega \in \Omega(n)$ $(n=0,1,2,\cdots)$ 及每个 $(a_1, a_2, \cdots, a_n) \in A^n$ 都有

$$f(\omega a_1 a_2 \cdots a_n) = \omega f(a_1) f(a_2) \cdots f(a_n),$$

（当 $n=0$ 时 $f(\omega_A) = \omega_B$），则称映射 f 为由 A 到 B 的**(代数)同态**((algebra)homomorphism).

定理 20.3.3 (1) 设 A, B, C 是三个 Ω 代数，$f: A \to B$，$g: B \to C$ 是两个同态，则 f 与 g 的复合 gf 是一个由 A 到 C 的同态.

(2) 1_A 是一个由 A 到 A 的同态.

(3) 以所有 Ω 代数为对象类，以它们间的同态为态射（箭）集的代数结构构成范畴 Ω-Alg（Ω 代数范畴）.

(4) 设 $\{A_\alpha \mid \alpha \in I\}$ 是 Ω 代数的标号族，$\prod_I A_\alpha$ 是例 20.2.5(2) 的族 $\{A_\alpha \mid \alpha \in I\}$ 的积，对每个 α 作 $P = \prod A_\alpha$ 到 A_α 中的射影映射

$p_\alpha: a \mapsto a_\alpha$，则 p_α 是 P 到 A_α 中的同态，因而 $\{P, p_\alpha\}$ 是集 $\{A_\alpha \mid \alpha \in I\}$ 的 Ω-alg 的积.

下面讨论同态的一些最重要的性质. 首先要利用同余关系在代数的元素间进行划分(分类)以构成商代数，然后研究原来的代数与商代数间的关系以及一些同态、同构的基本定理，可以看到它们是群、环、模、代数有关定理的推广.

定义 20.3.4 设 Φ 是 Ω 代数 A 上的等价关系，若它又是 $A\times A$ 的子代数，则称它为**同余关系**(congruence relation)，简称**同余**.

定义 20.3.5 设 A 是 Ω 代数，Φ 是它上面的一个同余，作商集 $A/\Phi=\{[a], a\in A\}$，其中 $[a]=\{a' \mid a'\in A, a'\Phi a\}$，并规定

对于 $\omega\in\Omega(n), n\geqslant 1, \omega[a_1]\cdots[a_n]=\omega[a_1\cdots a_n]$，

对于 $\omega\in\Omega(0), \omega_{A/\Phi}=[\omega_A]$，

则 A/Φ 关于所规定的运算构成一个 Ω 代数，称为 A 关于同余 Φ 的**商代数**(quotient algebra).

我们有以下重要定理：

定理 20.3.6 Ω 代数的同态基本定理 设 A 及 B 是两个 Ω 代数，f 是 A 到 B 的同态，则 $\Phi=f^{-1}f$ 是 A 上的同余而且其同态像 $f(A)$ 是 B 的子代数. 此外还存在 A/Φ 到 B 中的唯一同态 $\bar{f}$ 使 $f=\bar{f}\upsilon$，其中 υ 是 A 到 A/Φ 内的同态 $\upsilon: a \mapsto [a]$，且同态 $\bar{f}$ 是单射，而 υ 是满射.

因为 $A\sim A/\Phi$，运用基本定理可得.

定理 20.3.7 第一同构定理 设 Φ 是 Ω 代数 A 上的同余，A_1 是 A 的子代数，设 A_1' 是与 A_1 相交的各 Φ 等价类的并集，则 A_1' 是 A 的包含 A_1 的子代数. 令 $\Phi_1'=\Phi\cap(A_1'\times A_1')$ 及 $\Phi_1=\Phi\cap(A_1\times A_1)$ 分别是 A_1' 上的及 A_1 上的同余，而且映射 $[a_1]_{\Phi_1}\mapsto[a_1']_{\Phi'}$ 是 A_1/Φ_1 到 A_1'/Φ_1' 上的同构.

定理 20.3.8 设 A 是 Ω 代数，Φ 是 A 上的同余，A/Φ 是相应的

商代数，设 Θ 是 A 上的包含 Φ 的同余，$\Theta\supset\Phi$，换言之：

$$\forall a,b\in A,\quad a\Phi b\Rightarrow a\Theta b.$$

则必存在唯一的同态 $\nu_{\Theta/\Phi}:A/\Phi\to A/\Theta$ 使 $\nu_\Theta=\nu_{\Theta/\Phi}\nu_\Phi$，而且若用 Θ/Φ 表示 $\nu_{\Theta/\Phi}$ 的核，则 Θ/Φ 是 A/Φ 上的一个同余，映射 $\Theta\mapsto\Theta/\Phi$ 是 A 上包含 Φ 的同余集到 A/Φ 上的同余集上的双射．此外，对于 A 上包含 Φ 的两个同余 Θ_1 及 Θ_2 来说，则有 $\Theta_1\supset\Theta_2$ 当且仅当 $\Theta_1/\Phi\supset\Theta_2/\Phi$.

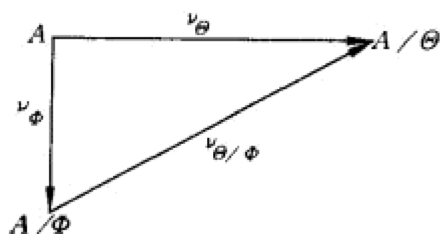


图 20.1

定理 20.3.9 第二同构定理 设 Θ 及 Φ 是 Ω 代数 A 上的两个同余：$\Theta\supset\Phi$，Θ/Φ 是定理 20.3.8 中的 A/Φ 的对应同余，则

$$[[a]_\Phi]_{\Theta/\Phi}\mapsto[a]_\Theta\qquad(a\in A)$$

是 $(A/\Phi)/(\Theta/\Phi)$ 到 A/Θ 上的同构.

为了加深对于上述各定理的认识，以它们在群与环中的原型为例作如下说明.

例 20.3.10 (1) 各定理在群范畴 Grp 中的原型．设 G 及 H 是两个群，f 是 G 到 H 内的同态，$K=f^{-1}(1)$ 是 G 的不变子群，核 $\Phi=f^{-1}f$ 是集 $\{(a,b)\mid a,b\in G,\ ab^{-1}\in K\}$，因而 $[a]_\Phi=aK=Ka$，而 G/Φ 即通常的商群 G/K，群的同态基本定理断言：$\bar{f}aK\mapsto f(a)$ 是 G/K 到 H 里的一个单态射且有分解 $f=\bar{f}\nu$，其中 ν 是满态射 $a\mapsto aK$．群的第一同构定理断言：若 H 是群 G 的子群，K 是 G 的不变子群，则由 H 及 K 生成的子群是 $HK=\{hk\mid h\in H,k\in K\}$，$K$ 在 HK 中及 $K\cap H$ 在 H 中均为不变子群，且有 HK/K 到 $H/(H\cap K)$ 上的同构

$$hk\mapsto h(H\cap K).$$

群的第二同构定理断言：若 H,K 都是 G 的不变子群且 $H\supset K$，则 H/K 是 G/K 的不变子群而且

$$gH\mapsto(gK)(H/K)$$

是 G/H 到 $(G/K)/(H/K)$ 上的同构.

(2) 各定理在环范畴 Ring 中的原型：环的同态基本定理断言：设 η 是环 R 到环 R' 中的同态，$K=\eta^{-1}(0')$ 是核，则 K 是 R 的一个理想且有唯一的 R/K 到 R' 中的同态 $\bar{\eta}$ 使 $\eta=\bar{\eta}\nu$，其中 ν 是 R 到 R/K 中的自然同态，而且 ν 是满态射，$\bar{\eta}$ 是单态射. 环的第一同构定理断言：设 R 是环，S 是子环，I 是 R 的理想，则 $S+I=\{s+i \mid s\in S, i\in I\}$ 是 R 的包含 I 作为理想的子环，$S\cap I$ 是 S 的理想，且有 $(S+I)/I$ 与 $S/(S\cap I)$ 间的同构：

$$s+I\mapsto s+(S\cap I), s\in S.$$

环的第二同构定理断言：若 η 是环 R 到环 R' 的满态射，K 是它的核，则在 $\langle R;+,0\rangle$ 的包含 K 的子群 H 的集与 R' 的与 H 用 $\eta(H)$ 配对的子群集的 1-1 对应中，H 是一个子环（理想）当且仅当 $\eta(H)$ 是 R' 的子环（理想）. 此外，若 I 是 R 的包含 K 的理想，则

$$a+I\rightarrow\eta(a)+I', I'=\eta(I)$$

是 R/I 与 R'/I' 间的同构.

(3) 除上二例外，在算子群中，环上的模中都可找到有关同态的相应定理.

20.4 同余格与子直积

本节将从格的角度探讨 Ω 代数上同余的重要性质，进而得出每个 Ω 代数都是子直积的不可约代数的子直积的重要结论(Birkhoff 定理).

定理 20.4.1 设 A 是 Ω 代数，$\Gamma(A)$ 是 A 上的所有同余构成的集，它以同余的包含关系 $\Theta\supset\Phi$（定理 20.3.8）作为偏序 $\geqslant$，则 $\langle\Gamma(A);\geqslant\rangle$ 是一个偏序集.

在得到以下各性质后可知 $\langle\Gamma(A);\geqslant\rangle$ 是一个完全格.

定理 20.4.2 设 $\{\Phi_\alpha\}$ 是 $\Gamma(A)$ 的子集，则

(1) $\bigcap \Phi_\alpha$ 仍是一个同余，且是$\{\Phi_\alpha\}$的 inf(最大下界)；

(2) 若$\{\Phi_\alpha\}$是被定向的，则$\bigcup \Phi_\alpha$ 也是同余；

(3) $A\times A$ 的子集 $A\times A$ 是同余，且是$(\Gamma(A);\geqslant)$的最大元，与它相应的商代数 $A/(A\times A)$则是平凡代数，即只含一个元素且其运算结果亦被完全确定的代数.

(4) 对角线关系 1_A(即$\forall a,b\in A,(a,b)\in 1\Rightarrow b=a$)是一个同余，商代数 $A/1_A\cong A$，因而可将 $A/1_A$ 与 A 等同.

定理 20.4.3 偏序集$\langle\Gamma(A);\geqslant\rangle$是完全格(定义 18.3.1).

定义 20.4.4 设 R 是 Ω 代数 A 上的二元关系，A 上包含 R 的一切同余的 inf(或交集)称为由 R 生成的同余，用$[R]$表示. 换言之，$[R]$是包含 R 的同余且被每个包含 R 的同余所包含.

还有极大同余概念.

定义 20.4.5 设 S 是偏序集 A 的子集，若在 S 中不存在异于 m 而能使 $s\geqslant m$ 的元 s，则元 m 称为 S 的**极大元**(maximal element).

对于极大同余有以下重要定理.

定理 20.4.6 设 a,b 是 Ω 代数 A 的两个相异元，$D(a,b)$是 A 上的同余 Φ 的集，这些 Φ 满足条件：$(a,b)\notin\Phi$，则 $D(a,b)$ 非空而且包含一极大元.

由此可得以下二推论.

推论 20.4.7 (1) 设 Θ 是 Ω 代数 A 上的一个同余，a 及 b 是能使$[a]_\Theta\neq[b]_\Theta$ 的两个元，则能使 $\Phi\supset\Theta$ 及$[a]_\Phi\neq[b]_\Phi$ 的同余 Φ 的集必包含一个极大元.

(2) 非零环 R 的任一真理想(单侧理想)必包含于一极大理想(单侧理想)之中.

为了解决 Ω 代数的构造问题，引入子直积及不可约的概念：

定义 20.4.8 设$\{A_\alpha|\alpha\in I\}$是 Ω 代数 A 的任一标号集，$P=\prod A_\alpha$，若存在 A 到 P 内的单态射 i 使得对于每个 α 都有 $i_\alpha=p_\alpha i$ 是 A_α 上的满射，则称 Ω 代数 A 是 A_α 的 **子直积** (subdirect

product).

例 20.4.9 (1) 整数环 **Z** 是域 $\mathbf{Z}/(p)$的子直积,这里 p 是任意素数.

(2) 设 A 是任一Ω 代数,$\{\Theta_\alpha \mid \alpha\in I\}$是 A 上所有能使$\bigcap\Theta_\alpha=1_A$ 的同余Θ_α 的标号集. 对每个 $\alpha\in I$ 作商代数 $A_\alpha=A/\Theta_\alpha$,并作积代数 $P=\prod_{\alpha\in I}A_\alpha$. 此时有 A 到 A_α 上的同态 $\nu_\alpha: a\mapsto[a]_{\Theta_\alpha}$ 及 A 到 P 内的同态 $\nu: a \mapsto[a]$,其中$[a_\alpha]=[a]_{\Theta_\alpha}$,$\nu$ 的核是偶对(a,b)的集,它对于$\forall\alpha\in I$ 有$[a]_\Theta=[b]_\Theta$,这是 ν_α 的核Θ_α 的交集,由于$\bigcap\Theta_\alpha=1_A$,ν 的核是 1_A 因而ν 是一个单态射. 由规定,对于任一α 来说,$\nu(A)$在 P 到 A_α 上的射影 p_α 下的象 $p_\alpha\nu(A)$是 A_α,所以 A 是 A_α 的一个子直积.

定义 20.4.10 设 A 是Ω 代数,若它的所有非 1_A 的同余的交集$\neq 1_A$,则称代数 A 是**子直积的不可约的**(subdirectly irreducible).

至此我们有

定理 20.4.11(Birkhoff 定理) 每个Ω代数A 都是一个子直积的不可约的代数的子直积.

20.5 正向极限与逆向极限

这是由代数族构造出来的两种新的代数结构,可以从任意范畴出发进行讨论,现在先给出几个预备概念.

定义 20.5.1 设 I 是一个集,$\leqslant$是其中的二元关系,若它满足自反律($\forall a\in I,a\leqslant a$)及传递律($a\leqslant b,b\leqslant c\Rightarrow a\leqslant c$),则称 I 为**拟序集**(pre-ordered set).

定义 20.5.2 设对象类 $\mathrm{ob}\mathscr{I}=I$,态射集为

$$\mathrm{hom}(a,b)=\begin{cases}\varnothing & (\text{若 } a\not\leqslant b),\\ \text{单独一个元} & (\text{若 } a\leqslant b),\end{cases}$$

的代数结构作成一范畴 $\mathscr{I}$,称为**拟序集范畴**(category of preodered set).

定义 20.5.3 由 $\mathscr{I}$ 到范畴 $\mathscr{C}$ 的函子是指映射 F,它使 $\forall \alpha \in I$, $\alpha \mapsto A_\alpha$ ($A_\alpha \in \mathrm{ob}\mathscr{C}$) 而使 $(\alpha,\beta) \mapsto \varphi_{\alpha\beta} \in \hom_{\mathscr{C}}(A_\alpha, A_\beta)$,其中偶对 (α,β) 满足 $\alpha \leqslant \beta$;而且此映射满足函子条件: $\varphi_{\alpha\gamma} = \varphi_{\beta\gamma}\varphi_{\alpha\beta}$ ($\alpha \leqslant \beta \leqslant \gamma$) 及 $\varphi_{\alpha\alpha} = 1_{A_\alpha}$.

下面给出正向极限的概念.

定义 20.5.4 设 $I = \{\alpha\}$ 是拟序集, $\mathscr{C}$ 是范畴, F 是由 $\mathscr{I}$ 到 $\mathscr{C}$ 的函子. $\mathscr{C}$ 的**正向极限**(direct limit) $\varinjlim (A_\alpha, \varphi_{\alpha\beta})$ 指的是集 $(A, \{\eta_\alpha\})$,其中 $A \in \mathrm{ob}\mathscr{C}$, $\eta_\alpha: A_\alpha \to A$, $\alpha \in I$,它满足 $\eta_\alpha = \eta_\beta\varphi_{\alpha\beta}$. 而且 $(A, \{\eta_\alpha\})$ 是通用的. 换言之: 如果 $(B, \{\zeta_\alpha\})$ 是另一集,则必存在唯一的态射 θ: $A \to B$ 使 $\zeta_\alpha = \theta\eta_\alpha$, $\alpha \in I$.

定理 20.5.5 如果范畴 $\mathscr{C}$ 的正向极限存在,则它必是唯一的.

例 20.5.6 Ω 代数的有限生成子代数的正向极限. 设 A 是 Ω 代数, I 是 A 的按包含关系定序的有限子集的集. 若 $F \in I$,令 A_F 为 A 的由 F 生成的子代数,而且若 $F \subset G$,则令 φ_{FG} 表示 A_F 到 $A_G (\supset A_F)$ 内的单射同态,显然 $\varphi_{FF} = 1_F$ 及 $\varphi_{GH}\varphi_{FG} = \varphi_{FH}$ ($F \subset G \subset H$). 此外,若 η_F 表示 A_F 到 A 内的单射同态,则 $\eta_G\varphi_{FG} = \eta_F$,现设 B 是 Ω 代数且 $\{\zeta_F \mid F \in I\}$ 是能使 $\zeta_F: A_F \to B$ 且满足 $\zeta_G\varphi_{FG} = \zeta_F$ ($F \subset G$) 的同态集,由于 φ_{FG} 是 A_F 到 A_G 内的单射,这表示 A_G 上的同态 ζ_G 是 A_F 上的 ζ_F 的扩张. 由于 $\bigcup A_F = A$,存在 A 到 B 中的唯一的同态 θ 使 $\zeta_F = \theta\eta_F$, ($F \in I$). 故 A 及 $\{\eta_F\}$ 构成正向极限 $\varinjlim (A_F, \varphi_{FG})$.

下面是 Ω 代数的构造定理.

定理 20.5.7 任一 Ω 代数都同构于有限生成代数的正向极限.

此外还有以下的存在定理.

定理 20.5.8 对于每个指标定向集 I, Ω 代数范畴 Ω-alg 中

必存在正向极限.

逆向极限是正向极限的对偶概念,所以可利用对偶原则得出相应的概念与结论.

定义 20.5.9 设 $I=\{\alpha\}$ 是拟序集. Ω-alg 是 Ω 代数范畴,F 是范畴 $\mathscr{I}$ 到 Ω-alg 的反变函子,因而有映射使 $\alpha\mapsto A_\alpha\in\mathrm{ob}\Omega$-alg$(\alpha\in I)$而且对于 $\alpha,\beta\in\mathscr{I}(\alpha\leqslant\beta)$有态射 $\varphi_{\beta\alpha}:A_\beta\to A_\alpha$ 使

$$\varphi_{\gamma\alpha}=\varphi_{\beta\alpha}\varphi_{\gamma\beta}\qquad(\alpha\leqslant\beta\leqslant\gamma),$$

$$\varphi_{\alpha\alpha}=1_{A_\alpha}.$$

则集$(A,\{\eta_\alpha\})$称为**逆向极限**(inverse limit),这里 $A\in\mathrm{ob}\Omega$-alg,$\eta_\alpha:A\to A_\alpha$ 满足条件:$\varphi_{\beta\alpha}\eta_\beta=\eta_\alpha(\alpha\leqslant\beta)$. 而且若$(B,\{\zeta_\alpha\})$是另一有上列性质的集:$B\in\mathrm{ob}\Omega$-alg,$\zeta_\alpha$:$B\to B_\alpha$ 满足条件 $\varphi_{\beta\alpha}\zeta_\beta=\zeta_\alpha(\alpha\leqslant\beta)$,则存在唯一的态射 $\theta:B\to A$ 使 $\eta_\alpha\theta=\zeta_\alpha\quad(\alpha\in I)$.

通常将逆向极限$(A,\{\eta_\alpha\})$记作

$$\varprojlim(A_\alpha,\varphi_{\alpha\beta}).$$

定理 20.5.10 若逆向极限存在,则它必是唯一的(在同构意义上).

例 20.5.11 Ω 代数逆向极限的构作法 在 Ω-alg 中各 A_α 是Ω 代数,$\varphi_{\beta\alpha}$是 A_β 到 A_α 内的同态$(\alpha\leqslant\beta)$. 为作出逆向极限代数,可先作积代数 $\prod A_\alpha$ 及射影 p_α:$\prod A_\alpha\to A_\alpha$,其中 $p_\alpha(a)=a_\alpha$,而 a 是$\alpha\mapsto a_\alpha(\in A_\alpha)$. 然后作

$$A=\{a\in\prod A_\alpha\mid p_\alpha(a)=\varphi_{\beta\alpha}p_\beta(a),\alpha,\beta\in I,\alpha\leqslant\beta\},$$

如果 A 是非空的(有可能 A 是空的,如此则逆向极限不存在),则可证原来的运算系在 A 内是封闭的,故 A 构成 $\prod A_\alpha$ 的一个子代数. 将它连同同态 $\eta_\alpha=p_\alpha|A$(p_α 在 A 上的限制)就能构成 Ω-alg 内的逆向极限$\varprojlim(A_\alpha,\varphi_{\alpha\beta})$.

例 20.5.12 Ω 代数逆向极限的另一构作法. 设给定的是代数 B 上的同余集$\{\Phi_\alpha\}$,按照 $\Phi_\alpha\supset\Phi_\beta$ 规定 $\alpha\leqslant\beta$,将集 $I=\{\alpha\}$ 拟序

化. 作 $A_\alpha = B/\Phi_\alpha$ 并对 $\alpha \leqslant \beta$ 使 $\varphi_{\beta\alpha}$ 为 A_β 到 A_α 内的同态 $\bar{b}_{\Phi_\beta} \mapsto \bar{b}_{\Phi_\alpha}$，则 $\varphi_{\alpha\alpha} = 1_{A_\alpha}$，$\varphi_{\beta\alpha}\varphi_{\gamma\beta} = \varphi_{\gamma\alpha}(\alpha \leqslant \beta \leqslant \gamma)$. 使 ν_α 表示 B 到 A_α 上的同态 $b \mapsto \bar{b}_{\Phi_\alpha}$，则 $\varphi_{\beta\alpha}\nu_\beta = \nu_\alpha(\alpha \leqslant \beta)$. 这蕴涵 $\varprojlim(A_\alpha, \varphi_{\alpha\beta}) = (A, \{\eta_\alpha\})$ 是存在的，由定义 20.5.9 知是唯一的.

下面介绍逆向极限的一个著名例子，它是由 Hensel 研究赋值论（valuation theory）时得到的.

例 20.5.13 p 进整数环. 设 p 是 $\mathbf{Z}$ 中的一个素数，(p^k) 是 p^k 的一切倍数所组成的主理想，并使 $k = 1, 2, 3, \cdots$. 设 Φ_k 是同余，它由 $a\Phi_k b \Leftrightarrow a \equiv b(\mathrm{mod}\, p^k)$ 确定，因此 $\mathbf{Z}/\Phi_k = \mathbf{Z}/(p^k)$ 是模 p^k 的同余类环. 若 $l \geqslant k$，则 $\Phi_l \subset \Phi_k$ 而且 $\bigcap \Phi_k = 1_{\mathbf{Z}}$. 现作各有限环 $\mathbf{Z}/(p^k)$ 的逆向极限，并称之为 p 进整数环 $\mathbf{Z}_p$. 它的一个元素是同余类（陪集）的一个序列 $(a_1 + (p), a_2 + (p^2), a_3 + (p^3), \cdots)$，其中 a_i 是整数而且对于 $l \geqslant k$，$a_k \equiv a_l(\mathrm{mod}\, p^k)$. 因此这个元素可用整数序列 $(a_1, a_2, \cdots)$ 表示. 两个序列 $(a_1, a_2, \cdots)$ 及 $(b_1, b_2, \cdots)$ 代表同一元素当且仅当 $a_k \equiv b_k(\mathrm{mod}\, p^k)$，$k = 1, 2, \cdots$. 两序列的加法和乘法可按照多项式方式进行. 若 $a \in \mathbf{Z}$，则可把它写成 $a = r_0 + r_1 p + \cdots + r_n p^n$，$(0 \leqslant r_i < p)$，因此 $(a_1, a_2, \cdots)$（其中当 $k \leqslant l$ 时 $a_k \equiv a_l(\mathrm{mod}\, p^k)$）可用 $(r_0, r_0 + r_1 p, r_0 + r_1 p + r_2 p^2, \cdots)(0 \leqslant r_i < p)$ 表示，这样就可将 $\mathbf{Z}_p$ 的任一元素与唯一确定的 p 进数：$r_0 + r_1 p + r_2 p^2 + \cdots (0 \leqslant r_i < p)$ 联系起来. 这些级数的加法与乘法对应于 $\mathbf{Z}_p$ 中的这些复合，因而归结为在 r_i 上作“复合”及“进位”，就像作多项式的加法和乘法一样，对位相加、交叉相乘.

20.6 超积

代数的超积与包含着关系与复合运算的一般结构在数理逻辑中占有重要的地位，因为任何基本命题若是对所有 A_α 都有效，则

对于 A_α 的每个超积也有效，超积首先被数理逻辑引入和应用. 有趣的是它对于代数学也是一个重要的工具，这在本节之末可以看到.

超积概念是建立在滤子及超滤子的概念之上的.

定义 20.6.1 设 B 是布尔代数，$F\subset B$，满足：

(1) 若 $a,b\in F$，则 $a\wedge b\in F$，

(2) 若 $a\in F$ 且 $b\geqslant a$，则 $b\in F$，

(3) $1_B\in F$，

则称 F 是 B 的**滤子**(filter).

定义 20.6.2 设 F 是布尔代数 B 的滤子，如果 $F\neq B$(或等价地 $0\notin F$)，则称 F 为 B 的**真滤子**(proper filter).

定义 20.6.3 设 F 是布尔代数 B 的真滤子，而且不被 B 的任何其他真滤子所包含(即 F 是 B 的极大真滤子)，则称 F 是 B 的**超滤子**(ultrafilter).

定理 20.6.4 B 的滤子 F 是超滤子当且仅当它是 B 的真滤子，而且对于任何 $a\in B$，a 或者它的补元 a' 至少有一个包含于 F 之中.

定理 20.6.5 布尔代数 B 的任一真滤子 F 均能嵌入一个超滤子之中.

定义 20.6.6 设 $\{A_\alpha\}$，$\alpha\in I$ 是 Ω 代数集，F 是幂集 $\mathscr{P}(I)$ 中的滤子(即若 $S_1,S_2\in F$，则 $S_1\cap S_2\in F$；若 $S\in F$ 及 $T\supset S$，则 $T\in F$)，作积代数 $\prod A_\alpha$ ，$\alpha\in I$ 并在其中规定关系 $\sim_F$ 如下：

$a\sim_F b\Leftrightarrow$ 标号集 $I_{a,b}=\{\alpha\in I\mid a_\alpha=b_\alpha\}\in F$，则可证明 $\sim_F$ 是代数 $\prod A_\alpha$ 上的同余，利用它作商代数 $\prod A_\alpha/\sim_F$ 并称之为 Ω 代数 A_α 的 ***F* 归纳积**(F-reduced product). 若 F 是超滤子，则 $\prod A_\alpha/\sim_F$ 称为 A_α 的**超积**(ultraproduct)；若所有的 A_α 都相等：$A_\alpha=A$，则称它为 A 的**超幂**(ultrapower).

作为例子及说明它在代数上的应用，有以下二定理.

定理 20.6.7 若干个除环(域)的超积仍为除环(域).

定理 20.6.8 设 R 是没有零因子的环,(因而是除环 D_a 的直积 $\prod D_a$ 的子环),则 R 可嵌入除环之中.

20.7 自由 Ω 代数

我们已讨论过由字母表生成的自由单元半群,本节将扩展到 Ω 代数中去. 由于由"字母表"生成的"字"未必都有"意义"(即不一定能执行原来代数系统中的运算),所以引发出鉴别一个"字"是否属于自由 Ω 代数的问题,由此可得到这个代数的"自由性".

定义 20.7.1 设 $\Omega=\bigcup_{n=0}^{\infty}\Omega(n)$ 是运算系,其中 $\Omega(n)$是 n 元运算集;设 X 是非空集,Y 是 Ω 及 X 的不相交并集,$Y=\Omega\,\dot{\cup}X$. 作积集 $Y^{(m)}=\{(y_1,y_2,\cdots,y_m)\mid y_i\in Y\}$,然后对 $m=1,2,\cdots$作所有积集的不相交并 $W(\Omega,X)=\dot{\bigcup}_{m=1}^{\infty}Y^{(m)}=\{(y_1,y_2,\cdots,y_m)\mid m\geqslant 1\}$.

在 $W(\Omega,X)$中规定**邻接乘法**(juxtaposition)如下:

$$(y_1,\cdots,y_m)(y_1',\cdots,y_r')=(y_1,\cdots,y_m,y_1',\cdots,y_r').$$

这个乘法显然满足结合律;此外对于 $\omega\in\Omega(0)$,使 Y 的一个固定元与它对应;对于 $\omega\in\Omega(n)$,$n\geqslant 1$,规定 ω 在$(w_1,w_2,\cdots,w_n)$ $(w_i\in W(\Omega,X))$上的运算结果为 $\omega w_1w_2\cdots w_n$,则 $W(\Omega,X)$构成 Ω 代数,称为**由 X 生成的 Ω 代数**,记为 $W(\Omega,X)$.

定义 20.7.2 定义 20.7.1 中的 Y 称为字母表,m 元组 $w=(y_1,y_2,\cdots,y_m)\in W(\Omega,X)$称为**字母表上的字**(word). 由于邻接乘法满足结合律以及为了简便,通常将$(y_1,y_2,\cdots,y_m)$简写成 $y_1y_2\cdots y_m$,而省去其中的括号和逗号.

为了便于鉴别,引人字的长度和价的概念.

定义 20.7.3 字 $w=y_1y_2\cdots y_m$ 中字母(包括元素的符号及运算符号)的个数 m 称为 w 的**长度**(lenght).

定义 20.7.4 字 w 给定后,它的**价**(valency)$v(w)$指的是:

(1) 若 $w=x\in X$,则 $v(x)=1$;

(2) 若 $w=\omega\in\Omega(n)$,则 $v(\omega)=1-n$;

(3) 若 $w=y_1y_2\cdots y_m$,则

$$v(w)=v(y_1y_2\cdots y_m)=\sum_1^m v(y_i).$$

例 20.7.5 $w=\omega_1^{(1)}\omega_2^{(1)}x_1\omega_3^{(2)}x_2x_3\omega_4^{(5)}$ 是一个字,各字母的上标分别表示运算的元数,其长度$=7$,价 $v(w)=(1-1)+(1-1)+1+(1-2)+1+1+(1-5)=-2$. 容易看出,该字是毫无“意义”的,就以最右端的 $\omega_4^{(5)}$ 来看,它是一个 5 元运算符号,要使它有“意义”除非在它的右边有 X 的 5 个元素. 但这里却没有,因此毫无“意义”可言.

为了保证字有“意义”,有以下定义.

定义 20.7.6 设 $F(\Omega,X)$是 Ω 代数 $W(\Omega,X)$的子代数,若对于集合 X 到 Ω 代数 A 内的任一映射 f 都能唯一地扩张成由 $F(\Omega,X)$到 A 内的同态 $\bar{f}$,则称 **$F(\Omega,X)$为 X 生成的自由代数**(free Ω-algebra generated by X).

根据映射的意义,该定义无异于说将 A 内的元代入 $F(\Omega,X)$内的“字”时可得 A 的一个元,也就是说这个“字”是“有意义”的.

当一个字给定后要判断它是否“有意义”,即它是否是自由代数 $F(\Omega,X)$的元,对此有以下的判定法.

定理 20.7.7 (1) 字 w 是 $F(\Omega,X)$的元当且仅当它能满足下述二条件:

1) $v(w)=1$;

2) w 的任一**右因子**(right factor)w'的价是正的. w 的右因子系指满足 $w=w''w'$的字 w'或者 w 自身.

(2) $F(\Omega,X)$的长度为 1 的子集是 $X\cup\Omega(0)$.

(3) 若 $w(\in F(\Omega,X))$的长度>1,则 w 的第一个字母是运算符 $\omega\in\Omega(n)$,$n\geqslant1$;而且 w 能唯一地表成 $\omega w_1w_2\cdots w_n$ 的形式,其

中 $w_i \in F(\Omega, X)$.

此定理可举例解释如下.

例 20.7.8 (1) 例 20.7.5 中的 $w_1 = \omega_1^{(1)} \omega_2^{(1)} x_1 \omega_3^{(2)} x_2 x_3 \omega_4^{(5)}$ 不是 $F(\Omega, X)$的元素，因为它的价 $v(w_1) = -2$.

(2) $w_2 = \omega_1^{(4)} x_1 x_2 x_3 \omega_2^{(2)} x_4 \omega_3^{(4)} x_5 x_6 \omega_4^{(0)} \omega_5^{(0)}$ 的价 $v(w_2) = 1$，它的第一个字母是运算符 $\omega_1^{(4)}$，要考虑它的各个右因子，可令 $u = x_1 x_2 x_3 \omega_2^{(2)} x_4 \omega_3^{(4)} x_5 x_6 \omega_4^{(0)} \omega_5^{(0)}$，然后由右向左作 u 的右因子 $u_i (1 \leqslant i \leqslant n)$，此处 u_i 是价为 i 的长度最大的右因子，现求 u_1：我们知道 $\omega_5^{(0)}$，$\omega_3^{(4)} x_5 x_6 \omega_4^{(0)} \omega_5^{(0)}$ 及 $\omega_2^{(2)} x_4 \omega_3^{(4)} x_5 x_6 \omega_4^{(0)} \omega_5^{(0)}$ 三个字的价都是 1，而长度最大的是第三个，故可令

$$u_1 = \omega_2^{(2)} x_4 \omega_3^{(4)} x_5 x_6 \omega_4^{(0)} \omega_5^{(0)}.$$

进而求 u_2：它是价为 2 的长度最大的右因子，显然 $u_2 = x_3 u_1$.

同理可得，$u_3 = x_2 u_2$，$u_4 = x_1 u_3 = u$.

这些右因子 u_1, u_2, u_3, u_4 的价分别为 1,2,3,4，据定理 20.7.7(1) 知，w_2 是 $F(\Omega, X)$的元素.

(3) $F(\Omega, X)$的长度为 1 的元只能是 $x (x \in X)$ 或 $\omega \in \Omega(0)$，因此得定理 20.7.7(2).

(4) 设 $w \in F(\Omega, X)$，若其长度>1，据例 20.2.5(2)即知其第一个字母是 $\omega \in \Omega(n)$，$n \geqslant 1$.

在此定理的基础上即可证以下定理.

定理 20.7.9 $\boldsymbol{F(\Omega, X)}$**的自由性** 设 f 是 X 到 Ω 代数 A 的映射，则 f 可唯一地扩展成 $F(\Omega, X)$到 A 内的一个同态 $\bar{f}$.

此定理也可用范畴论的语言表达如下.

定理 20.7.10 设 F 是由范畴Ω-alg 到 Set 的忘却函子，它将每个 Ω 代数射入其基集，而将代数同态射入相应的集的映射. 若 X 是任一非空集，i 是 X 射入 $F(\Omega, X)$的单射，则偶对$(F(\Omega, X), i)$构成由 X 到函子 F 的通用结构，从而同态扩张 $\bar{f}$ 是唯一的.

20.8 簇

自由Ω代数解决了"字"的"意义"问题，保证了它里面的元可以进行原来系统中的各种运算；本节将考虑它里面的等式，并称满足某些等式的Ω代数类为簇，我们要研究它所具有的某些简单性质.

定义 20.8.1 设$F(\Omega,X)$是由集X生成的自由Ω代数，(w_1,w_2)是它的元素的偶对，A是Ω代数，f是$F(\Omega,X)$到A内的任一同态. 若对于每个f都有$f(w_1)=f(w_2)$，则称Ω代数A满足等式$w_1=w_2$，或称$w_1=w_2$是A的**规律**(law).

定义 20.8.2 设S是$F(\Omega,X)\times F(\Omega,X)$的子集，若对于每个$(w_1,w_2)\in S$，$\Omega$代数类的每个成员都满足等式$w_1=w_2$，则称它为**由$S$确定的$\Omega$代数簇**(variety)，用$V(S)$表示.

例 20.8.3 (1) 群簇(variety of groups). 设$\Omega=\{\omega^{(2)},\omega_1^{(1)},\omega_2^{(0)}\}$，$X=\{x_1,x_2,x_3\}$，则群的类由$F(\Omega,X)\times F(\Omega,X)$的下列五个偶对集规定：

$(\omega^{(2)}\omega^{(2)}x_1x_2x_3,\omega^{(2)}x_1\omega^{(2)}x_2x_3)$,

$(\omega^{(2)}\omega^{(0)}x_1,x_1)$,

$(\omega^{(2)}x_1\omega^{(0)},x_1)$,

$(\omega^{(2)}x_1\omega^{(1)}x_1,\omega^{(0)})$,

$(\omega^{(2)}\omega^{(1)}x_1x_1,\omega^{(0)})$.

若将Ω代数A的三个运算$\omega^{(2)},\omega_1^{(1)},\omega_2^{(0)}$分别表成"$\cdot$","$^{-1}$",及"1"(单元)，$X$中的$x_1,x_2,x_3$分别用$a,b,c$表示，则上列五个偶对集分别是以下五条规律：

$$(a\cdot b)\cdot c=a\cdot(b\cdot c),$$
$$1\cdot a=a,$$
$$a\cdot 1=a,$$

$$a \cdot a^{-1} = 1,$$

$$a^{-1} \cdot a = 1.$$

A 满足这五个等式，所以是群，因而 $V(S)$ 是群簇.

(2) 仿上可作单元半群、格、环、交换代数、布尔代数等的簇.

定理 20.8.4 任一 Ω 代数簇均满足以下"闭包性质"(closure properties)：

(1) 若 $A \in V(S)$，则 A 的任一子代数必包含于 $V(S)$ 之中.

(2) 若 $A \in V(S)$，则 A 的每个同态象 $\bar{A}$ 必包含于 $V(S)$ 之中.

(3) 设 $\{A_\alpha | \alpha \in I\}$ 是包含于 $V(S)$ 的代数的标号集，则 $\prod A_\alpha \in V(S)$.

这是很明显的，因为如果以 p_α 表示 $A = \prod A_\alpha$ 到 A_α 内的射影，而令 f 为 $F(\Omega, X)$ 到 A 内的同态，则对于每个 $(w_1, w_2) \in S$ 都有 $p_\alpha f(w_1) = p_\alpha f(w_2)$，因而 $f(w_1) = f(w_2)$，故 $A \in V(S)$.

该定理的逆命题亦成立.

定理 20.8.5 Birkhoff 定理 Ω 代数的一个类是一个簇的充要条件是它具有定理 20.8.4 中的闭包性质(1)，(2)，(3).



数理逻辑

数理逻辑又称符号逻辑.是用数学方法研究数学思维模型的科学.它把数学的推理方法及其使用的语言作为研究的对象,应用数学方法(特别是形式化方法)加以研究.它使用形式语言(人造符号语言)来表达思维的形式结构和规律,把对思维规律的研究变换为对符号规律的研究.它既是数学,也是逻辑学.国际数学界把它列入"核心数学"(纯数学),逻辑学界称它为现代逻辑.

数理逻辑是边缘性学科,应用范围极为广阔,它既应用于自然科学的物理学、化学、生物学,又与社会科学如哲学、伦理学、语言学、心理学、经济学、法学、文学以及历史科学均有联系.并广泛应用于计算机科学,信息科学及管理科学.

一般认为德国数学家莱布尼兹(G. W. Leibniz,1646—1716)与英国数学家布尔(G. Boole,1815—1864)均为数理逻辑的创始人.

它的发展大致可分为四个阶段.

第一阶段,从 17 世纪 70 年代,莱布尼兹首次提出数理逻辑的设想到 19 世纪末叶布尔的工作.这时开始运用数学方法研究形式逻辑,初步完成了命题演算(布尔代数),同时建立了关系逻辑.

第二阶段,从 19 世纪 70 年代到 20 世纪 30 年代,这时为了加深理解数学命题的实质和数学思维的规律,开始建立了形式化的命题演算和谓词演算,突破了古典形式逻辑的局限性.

第三阶段,从 20 世纪 30 年代到 50 年代是数理逻辑的巅峰时代,这一时期最重要的成果是:

(1) Gödel 完全性定理与不完全性定理.

(2) Tarski 的形式语言的真理论.

(3) Turing 机器理论与判定问题.

第四阶段,20 世纪 50 年代以后,在先前理论基础与计算机发展的刺激下,数理逻辑得到了加速的发展,在基础性的逻辑演算方面除了标准/古典逻辑演算(标准命题演算和谓词演算)外,非标准逻辑演算得到了迅速的发展,例如多值逻辑、模糊逻辑、直觉主义逻辑以及模态逻辑、时态逻辑等,并且形成了四大分枝:公理集合论、模型论、证明论与递归论.



21 标准(古典)命题逻辑

21.1 命题符号化

数理逻辑是研究“数学思维”的数学模型，数学思维是一种精确的思维，它的思维规律是日常生活和大多数科学领域中进行推理的可靠依据. 历史上，最初研究这种思维规律的传统逻辑，是借助于自然语言来研究的. 由于自然语言是人们交流思想的一种工具，它既要能表达严密精确的思维，又要能表达含糊不清的思想. 又由于它的广泛性，易变性与多义性，不适用于研究严格的推理规律，因此遇到了不可克服的困难. 数理逻辑利用数学方法，特别是形式化的方法，建立了严格的形式推理系统，深刻地研究了这种思维规律，取得了极大的成功. 有人说，数理逻辑既是逻辑的数学，又是数学的逻辑，是传统逻辑的现代化，是现代化的传统逻辑.

为了研究推理，首先要研究判断. 判断总是用陈述句来表示的. 能够分辨真假的语句，其内涵称作**命题**(proposition). 因此只有陈述句可以用来表示命题，而感叹句、疑问句、命令句都不是命题.

由简单陈述句表示的命题称作**简单命题**或**原子命题**(simple proposition/atomic proposition). 由复杂陈述句(或复合句)表示的命题称作**复合命题**或**分子命题**(composite proposition/molecular proposition)，无论是哪一种命题，在数理逻辑中都要用“符号”来表示.

对于最简单的命题，通常以大写的或带有下标的拉丁字母表示：$A, B, C, \cdots, P, Q, R, \cdots, (A_i, B_i, C_i, \cdots, P_i, Q_i, R_i, \cdots)$. 有些

文献中也常用小写字母来表示.

为了保证符号的单一性,对于不同的命题,必须用不同的符号.

为了把复杂命题形式化,还要把自然语言中表示逻辑性质的联结词用符号来表示. 把复杂的命题看成是由原子命题通过逻辑联结词"构造"出来的数学公式.

21.2 命题联结词,真值表

数理逻辑中常用的逻辑联结词有 5 种,表示如下:

非(并非)	¬(~/NOT)	(否定词)
并且(而且)	∧(&/AND)	(合取词)
或(或者)	∨(OR)	(析取词)
若…则… 如果…那么…	→(IF…THEN…)	(条件词/蕴含词)
当且仅当	↔(≡/Iff)	(双条件词/等值词)

上述第一列所表示的是该逻辑联结词在自然语言(汉语)中的基本涵义,第二列表示它的符号,第三列是它的名称. 利用这些联结词,就可以表示比较复杂的命题.

例 21.2.1 把下列命题符号化

(1) 北京是中国的大城市.(P).

(2) 北京不是中国的大城市.($\neg P$).

(3) 塑料不是金属.(Q).

(4) 塑料是金属.($\neg Q$).

例 21.2.1 中(1)是一个原子命题. (2)是一个稍微复杂一些的命题,它不能仅由一个符号表示,而要由原子命题 P 与联结词 ¬ 的组合 $\neg P$ 表示出来. (3) 究竟算不算是原子命题,有不同的看法,有些文献认为原子命题中不能包含联结词,(3) 中"隐含"有

联结词“$\neg$”的涵义，因此它不应当算作原子命题；然而也有人认为，在人们发现塑料之初，对它的性质还不够了解时，命题(3)也是一种肯定的判断，虽然这种肯定是“隐含”着某种否定的涵义加以表达的. 这个问题，我们不去争论. 重要的在于，如果命题(3)用 Q 表示，那么命题(4)就应该用 $\neg Q$ 表示.

例 21.2.2 把下列命题符号化

(1) 今天下雨. (P).

(2) 教室里有两张桌子. (Q).

(3) $2+3=5$. (R).

(4) 今天下雨而且教室里有两张桌子. ($P\wedge Q$).

(5) 今天不下雨并且 $2+3=5$. ($\neg P\wedge R$).

在自然语言中，联结词“并且”，多半用来表示两种同类事物的并存. 而本例中的(4)与(5)有点使人奇怪，每个语句中的两个并列子句，在含意上毫不相干. 这是因为在数理逻辑中只考虑两个命题之间的形式关系，而不顾及语句的含义，正如我们在研究语法规则时，只考虑句子的形式，而不考虑句子的意义. 值得注意的是，像 $2+3=5$ 这样的数学公式也是一个命题. 事实上，一个完整的数学公式，与一个完整的陈述句并没有什么本质的差异.

例 21.2.3 把下列命题符号化

(1) 今晚我看电视. (P).

(2) 今晚我开会. (Q).

(3) $3\leqslant 2$. (R).

(4) 今晚我看电视或者我开会. ($P\vee Q$).

(5) 3 不大于 2 或我开会. ($R\vee Q$).

在例 21.2.3 中(4)，(5)两个语句都使用了“或”，但仔细分析起来，这两种“或”的逻辑意义是不一样的. 语句(4)的意思是：要么我看电视，要么我去开会. 这两件事不能同时去做，这里的“或”是含有“二者择一”的意思，一般称为“不可兼或”. 而语句(5)中的

"或",二者并没有互相排斥的意思,称之为"可兼或".我们所说的析取词,它的逻辑意义是指"可兼或".为了区分这两种联结词,"可兼或"总是用"$\vee$"来表示,而"不可兼或"有时用"$\overline{\vee}$",有时又用"$\oplus$"来表示.

"可兼或"的逻辑意义在自然语言与数学语言中也略有差异.例中的(5)是兼顾到数学上的需要,允许在内容上毫不相干的语句也可以用析取词加以联结.

例 21.2.4 把下列命题符号化

(1) 河水泛滥.(P).

(2) 庄稼被毁坏.(Q).

(3) 雪是黑的.(R).

(4) 如果河水泛滥,那么庄稼被毁坏.($P \to Q$).

(5) 如果河水泛滥,那么雪是黑的.($P \to R$).

(6) 如果雪是黑的,那么河水泛滥.($R \to P$).

关于条件词,在自然语言中有极为繁多的表达方式,但它的主要涵义是:如果前提 P 真,那么结论 Q 必真(即 Q 不会假);换言之,绝对不会发生前提真而结论假的事情.这就是条件词大量出现在有关推理的场合.然而在自然语言中若 P 则 Q 还表示 P 是 Q 的原因,这种因果相依的紧密联系,由于过分广泛还不能完全地反映在条件词中.条件词仅仅反映了在推理过程中前提与结论间的真假关系.

例 21.2.5 把下列命题符号化

(1) $\triangle ABC$ 是等边三角形.(P).

(2) $\triangle ABC$ 是等角三角形.(Q).

(3) $\triangle ABC$ 是等边三角形当且仅当$\triangle ABC$ 是等角三角形.($P \leftrightarrow Q$).

双条件词，在自然语言中相当于"当且仅当"，它所联结的两个命题是逻辑上"等值"的(即取相同的"真"，"假"值)，因此有时也称为等值词.

从上面的例子可以看出，通过原子命题及联结词可以构成更加复杂的命题；反过来说，一些复杂的命题也可以通过简单的原子命题及联结词表达出来.

正如数学中的变量一样，我们要定义命题变量.

定义 21.2.6 不确指的命题，称为**命题变量**(propositional variable)，它的变域是原子命题集.

有些文献中，用小写拉丁字母表示命题变量：$p,q,r,\cdots$而用大写字母表示具体的、确指的命题：$P,Q,R,\cdots$(确指的命题有时也称为**命题常量**(propositional constant). 本书在不发生混淆的情况下有时也用大写字母表示命题变量.

原子命题在不确指时称为命题变量，而复合命题是由原子命题与联结词构成的命题，因而是命题变量的"函数". 不过这种函数所取的"值"不像传统数学中的数值，而是"真"，"假"值. 今后我们也称上述的逻辑联结词为**真值函数**(truth value function). 仿照数学中的列表法，对由联结词构成的函数，列出表 21.1～表 21.5，称之为**真值表**(truth table).

表 21.1

P	$\neg P$
$\top$	$\bot$
$\bot$	$\top$

表 21.2

P	Q	$P\wedge Q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

表 21.3

P	Q	$P\vee Q$
⊤	⊤	⊤
⊤	⊥	⊤
⊥	⊤	⊤
⊥	⊥	⊥

表 21.4

P	Q	$P\leftrightarrow Q$
⊤	⊤	⊤
⊤	⊥	⊥
⊥	⊤	⊥
⊥	⊥	⊤

表 21.5

P	Q	$P\rightarrow Q$
⊤	⊤	⊤
⊤	⊥	⊥
⊥	⊤	⊤
⊥	⊥	⊤

在上述表中，我们用“⊤”、“⊥”分别代表“真”、“假”二值（有些文献中用“t”、“f”或用“1”、“0”分别代表“真”、“假”二值）．由联结词“$\wedge$”所定义的真值函数，既可以用真值表 21.2 来表达，也可以由公式 $P\wedge Q$ 来表达．由表 21.1～表 21.4 对由联结词所定义的函数，是明白无误的．值得注意的是，由表 21.5 所定义的真值函数常常会引起读者的疑虑，不少读者以为当命题 P 为假，命题 Q 为真时，$P\rightarrow Q$ 怎么会为真呢？哪有前提假，结论真时：“如果 P 那么 Q”反而会取真值？这主要是由于人们经常把 $P\rightarrow Q$ 理解作：原因→结果时导致的误解．事实上，我们已经说过联结词“→”只能保证前提为真时，它的结论必真．它不能完全表达原因与结果的种种复杂联系．

21.3 其他联结词

在命题逻辑中，除去前述的逻辑联结词外，还有其他的联结词，分述如下：

定义 21.3.1 不可兼或“$\overline{\vee}$”（在逻辑电路中常称为“**异或门**”，有时用符号$\oplus$表示．

它的真值表是表 21.6．

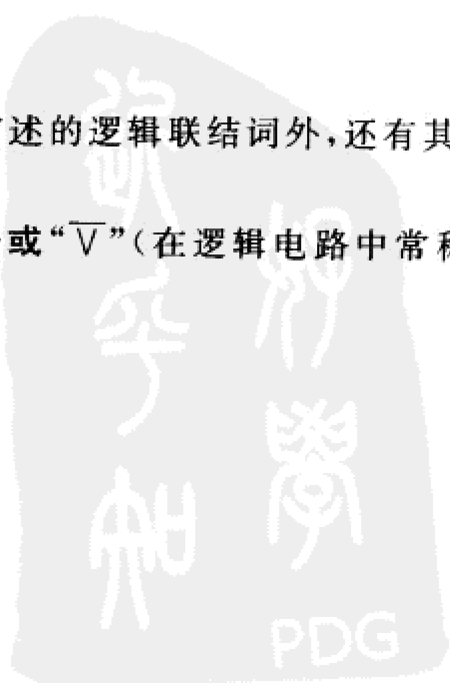


表　21.6

P	Q	$P\overline{\vee}Q$
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

在等价变换之下，有下面的基本性质：

(1) $P\overline{\vee}Q \Leftrightarrow Q\overline{\vee}P$.　　(交换律)

(2) $(P\overline{\vee}Q)\overline{\vee}R \Leftrightarrow P\overline{\vee}(Q\overline{\vee}R)$.　　(结合律)

(3) $P\wedge(Q\overline{\vee}R) \Leftrightarrow (P\wedge Q)\overline{\vee}(P\wedge R)$.　　(分配律)

(4) $P\overline{\vee}Q \Leftrightarrow (P\wedge\neg Q)\vee(\neg P\wedge Q)$.

(5) $P\overline{\vee}Q \Leftrightarrow \neg(P\leftrightarrow Q)$.

性质(4)，(5)指出联结词$\overline{\vee}$与其他联结词之间的联系，它表明可以把含有逻辑联结词$\overline{\vee}$的公式，通过联结词$\neg$，$\vee$，$\wedge$，$\rightarrow$，$\leftrightarrow$表达出来.

定义 21.3.2　**sheffer 竖**“$\uparrow$”(在逻辑电路中常称为“与非门”，有时也记作 NAND(=NOT−AND))．$P\uparrow Q \triangleq \neg(P\wedge Q)$.

联结词$\uparrow$一般满足交换律，不满足结合律．与其他联结词的关系有：

(1) $P\uparrow P \Leftrightarrow \neg P$.　　(自反否定律)

(2) $(P\uparrow Q)\uparrow(P\uparrow Q) \Leftrightarrow P\wedge Q$.

(3) $(P\uparrow P)\uparrow(Q\uparrow Q) \Leftrightarrow P\vee Q$.

(4) $P\uparrow(Q\uparrow R) \Leftrightarrow \neg P\vee(Q\wedge R)$.

(5) $(P\uparrow Q)\uparrow R \Leftrightarrow (P\wedge Q)\vee\neg R$.

定义 21.3.3　**Pierce 箭**“$\downarrow$”(在逻辑电路中称作或非门，有时记作 NOR(=NOT−OR)．$P\downarrow Q \triangleq \neg(P\vee Q)$.

联结词 $\downarrow$ 一般满足交换律，不满足结合律. 与其他联结词之间的关系有：

(1) $P \downarrow P \Leftrightarrow \neg P$. (自反否定律)

(2) $(P \downarrow Q) \downarrow (P \downarrow Q) \Leftrightarrow P \vee Q$.

(3) $(P \downarrow P) \downarrow (Q \downarrow Q) \Leftrightarrow P \wedge Q$.

(4) $P \downarrow (Q \downarrow R) \Leftrightarrow \neg P \wedge (Q \vee R)$.

(5) $(P \downarrow Q) \downarrow R \Leftrightarrow (P \vee Q) \wedge \neg R$.

由定义 21.3.2 及定义 21.3.3 可以看出，联结词 $\uparrow$ 与 $\downarrow$ 均不满足结合律. 从传统数学看，有些文献认为这是一个缺点. 然而从计算机科学的观点看，这恰恰是一个优点，它说明使用这两种联结词表达的逻辑电路不仅可以反映电路的逻辑性质，还可以反映电路的“时序性”.

定义 21.3.4 联结词 IF-THEN-ELSE(广泛用于程序语言中的联结词).

IF P THEN Q ELSE $R \triangleq (P \rightarrow Q) \wedge (\neg P \rightarrow R)$.

这个联结词有下面的性质：

(1) IF $\neg A$ THEN B ELSE $C \Leftrightarrow$ IF A THEN C ELSE B.

(2) IF T THEN B ELSE $C \Leftrightarrow$ IF $\perp$ THEN C ELSE $B \Leftrightarrow B$.

(3) IF B THEN $\perp$ ELSE $\top \Leftrightarrow \neg B$.

(4) IF B THEN C ELSE $C \Leftrightarrow$ IF $\perp$ THEN B ELSE $C \Leftrightarrow C$.

定义 21.3.4 中的三元联结词 IF-THEN-ELSE，其含义是：若……则……否则……，它的真值表如表 21.7.

表 21.7

P	Q	R	IF P THEN Q ELSE R
⊤	⊤	⊤	⊤
⊤	⊤	⊥	⊤
⊤	⊥	⊤	⊥
⊤	⊥	⊥	⊥
⊥	⊤	⊤	⊤
⊥	⊤	⊥	⊥
⊥	⊥	⊤	⊤
⊥	⊥	⊥	⊥

从上述定义可以看到,这些新的联结词不外乎是由 5 大联结词的适当组合构成的,它们在应用领域中大量出现.

21.4 联结词的功能完备集(完全集)

同一个真值函数可以用各种联结词构成种种不同形式的表达式,任意一个真值函数一定可以通过命题变量与 5 种联结词组成的公式表示出来.

不仅如此,对于任何含有条件词及双条件词的真值函数,可以仅仅应用联结词 $\neg, \wedge, \vee$ 就足够了.

$P \to Q \Leftrightarrow \neg P \vee Q$.

$P \leftrightarrow Q \Leftrightarrow (\neg P \vee Q) \wedge (\neg Q \vee P)$.

换言之,为了表达全部真值函数,并不一定需要全部的 5 种联结词: $\neg, \wedge, \vee, \to, \leftrightarrow$. 这就产生了联结词的功能完备集的问题.

定义 21.4.1 设 $\mathscr{C}$ 是联结词的集合,若对于任意一个真值函数,均存在一个与之等价的真值函数,而后者仅含有 $\mathscr{C}$ 中的联结

词,则称 $\mathscr{C}$ 是联结词的**功能完备集**(完全集)(adequate set of connectives).

在理论上与应用上通过选用不同的功能完备集,可以更方便地对真值函数类进行研究.

定理 21.4.2 下述联结词集合都是功能完备集:

(1) $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$.

(2) $\{\neg, \vee, \wedge, \rightarrow\}$.

(3) $\{\neg, \vee, \wedge, \leftrightarrow\}$.

(4) $\{\neg, \vee, \rightarrow, \leftrightarrow\}$.

(5) $\{\neg, \wedge, \rightarrow, \leftrightarrow\}$.

(6) $\{\neg, \vee, \rightarrow\}$.

(7) $\{\neg, \wedge, \leftrightarrow\}$.

(8) $\{\neg, \vee, \leftrightarrow\}$.

(9) $\{\neg, \wedge, \rightarrow\}$.

(10) $\{\neg, \rightarrow, \leftrightarrow\}$.

(11) $\{\neg, \rightarrow\}$.

(12) $\{\neg, \vee, \wedge\}$.

(13) $\{\neg, \vee,\}$.

(14) $\{\neg, \wedge\}$.

(15) $\{\neg, \vee, \wedge\}$.

(16) $\{\overline{\vee}, \wedge\}$ ($\{\oplus, \wedge\}$).

(17) $\{\uparrow\}$.

(18) $\{\downarrow\}$.

(19) {IF-THEN-ELSE}.

注 21.4.3 (1) 本来在上述定理中,功能完备集应表示成 $\mathscr{C}\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$,为了简洁,可省去字母 $\mathscr{C}$,而直接记作 $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$.

(2) 上述定理给出许多功能完备集,这些功能完备集在各种

不同的场合出现.

首先{$\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$}是最常用的功能完备集，在任何场合都是适用的. 完备集{$\neg$, $\wedge$, $\vee$}是一个重要的功能完备集，使用该集来表达的真值函数系统，常称为 Boole 代数系统. 然而使用功能完备集{$\oplus$, $\wedge$}来表示真值函数系统，也是一种 Boole 代数系统，这种系统经常在编码理论中出现(其中"$\oplus$"称为"对位布尔和"，"$\wedge$"称为"布尔积"). 另外在研究逻辑系统的演绎与推理时，{$\neg$, $\rightarrow$}是一个重要的功能完备集. 在制造大规模集成电路的芯片中完备集{$\uparrow$}，{$\downarrow$}有广泛的应用. 在程序系统的理论研究中，仅含一个联结词的功能完备集{IF-THEN-ELSE}也很有用.

21.5 命题形式与等价(等值)演算

21.5.1 命题形式(合式公式)

由原子命题与逻辑联结词可以构成复合命题，使用命题变量与联结词可以构成复合命题形式，也就是真值函数，它的递归定义如下：

定义 21.5.1 一个含有命题变量和联结词的符号表达式，若满足以下规则，则称为**命题形式**(propositional formula)(或称为**合式公式**(well formed formula/简记为 wff)：

(1) 任何命题变量本身(包括"真"，"假"值$\top$, $\bot$)是命题形式.

(2) 如果 $\mathscr{A}$ 和 $\mathscr{B}$ 是命题形式，那么$(\neg\mathscr{A})$, $(\mathscr{A}\wedge\mathscr{B})$, $(\mathscr{A}\vee\mathscr{B})$, $(\mathscr{A}\rightarrow\mathscr{B})$和$(\mathscr{A}\leftrightarrow\mathscr{B})$是命题形式.

(3) 命题形式仅由有限次使用规则(1)，(2)产生.

注 (1) 上述定义是一种递归定义，它同时指出了在一个命题形式的构造过程中符合(1)，(2)的任意一步所得到的都是命题形式，它们称为终结命题形式的**子公式**(sub formula).

(2) 在命题逻辑中，命题形式，命题公式，合式公式都是同义词.

(3) 在本书中常用花体字母：$\mathscr{A},\mathscr{B},\mathscr{C},\cdots$表示命题形式或真值函数，它们都是命题变量的函数.

例 21.5.2 说明$((P\wedge Q)\rightarrow(\neg(Q\vee R)))$是命题形式.

根据定义 21.5.1 中的条件(1)，P,Q,R 是命题形式，根据条件(2)，$(P\wedge Q)$和$(Q\vee R)$是命题形式. 再根据条件(2)知$(\neg(Q\vee R))$是命题形式. 最后根据条件(2)，$((P\wedge Q)\rightarrow(\neg(Q\vee R)))$是命题形式.

对于较长的表达式判断其是否是命题形式，有时是困难的. 下面介绍一种从图论来的方法. 从图论的观点看，每一个命题公式都可以用一棵“树”来表示，其中“树”的“结点”与联结词对应，而“树叶”则对应于命题变量，例如，公式

$$((P\wedge R)\rightarrow((\neg Q)\vee(S\leftrightarrow Q)))$$

就可以用一棵“树”表示如图 21.1

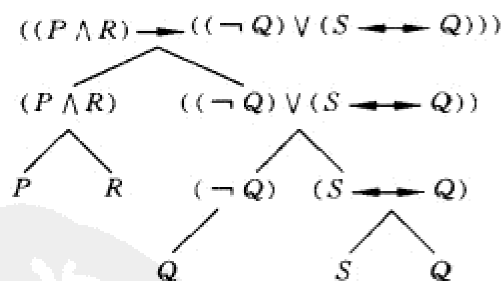


图 21.1

我们也可以反过来说，凡是不能用“树”来表示的表达式，一定不是命题公式.

联结词：$\neg,\wedge,\vee,\rightarrow,\leftrightarrow$决定简单的真值函数. 使用这些联结词的真值表，可以对任何给定的命题形式构造真值表. 真值表是一个命题形式(真值函数)的图表表示. 函数自变量的个数就是

命题形式中命题变量的个数.

一般情况下,对于一个含有 n 个不同命题变量的命题形式,它是 n 元函数,真值表有 2^n 行,对应于命题变量值的每一种可能组合占有一行,对应于有 2^n 行的真值表的最后一列中$\top$和$\bot$的 2^{2^n} 种可能的排列方式,可知有 2^{2^n} 个不同的 n 元真值函数. 用 n 个命题变量可能构造的命题形式的数目显然是无限的,因此可知,不同的命题形式可以对应于同一个真值函数.

例 21.5.3 构造命题形式$((\neg P)\vee Q)$的真值表 21.8.

表 21.8

P	Q	$\neg P$	$((\neg P)\vee Q)$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$

从表 21.8 可以看出,相应于这个命题形式的真值函数,与命题形式$(P\to Q)$所确定的真值函数是相同的.

定义 21.5.4 (1) 恒取真值的命题公式称为**永真公式**(或**重言式**/tautology).

(2) 恒取假值的命题公式称为**永假公式**(或**矛盾式**/contradication).

例 21.5.5

(1) $(P\vee\neg P)$是重言式.

(2) $(P\wedge\neg P)$是矛盾式.

(3) $(P\leftrightarrow(\neg(\neg P)))$是重言式.

(4) $((\neg P\to Q)\to(((\neg P)\to(\neg Q))\to P))$是重言式.

证实一个命题形式是否是重言式或矛盾式,可靠的方法是构造它的真值表.

从定义 21.5.4 可知，一切含有 n 个命题变量的重言式给出同一个 n 元真值函数，它总是恒取 $\top$ 值，因此也称它所表示的函数为**永真函数**. 由矛盾式表示的函数，称为**永假函数**.

21.5.2 命题等值式(等价式)

如前所述，不同的命题形式可以对应于同一个真值函数. 有下面的例子.

例 21.5.6 命题公式 $(\neg(P\wedge Q))$ 与命题公式 $((\neg P)\vee(\neg Q))$ 表示同一个真值函数.

分别给出它们的真值表，就一目了然.

表 21.9

P	Q	$\neg(P\wedge Q)$
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

表 21.10

P	Q	$(\neg P)\vee(\neg Q)$
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

命题公式 $(\neg(P\wedge Q))\leftrightarrow((\neg P)\vee(\neg Q))$ 的真值表，见表 21.11.

表 21.11

P	Q	$(\neg(P\wedge Q))\leftrightarrow((\neg P)\vee(\neg Q))$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

从例 21.5.6 可知，如果两个命题公式 $\mathscr{A},\mathscr{B}$ 表示同一个真值

函数,那么命题公式:$\mathscr{A}\leftrightarrow\mathscr{B}$ 表示一个永真函数(换言之,$\mathscr{A}\leftrightarrow\mathscr{B}$ 是一个重言式).

定义 21.5.7 设 $\mathscr{A},\mathscr{B}$ 是命题形式,若$(\mathscr{A}\leftrightarrow\mathscr{B})$是重言式,称 $\mathscr{A}$ **逻辑等价** $\mathscr{B}$(logically equivalent). 若$(\mathscr{A}\rightarrow\mathscr{B})$是一个重言式,则称 $\mathscr{A}$ **逻辑蕴含** $\mathscr{B}$(logically implies). 分别记作 $\mathscr{A}\Leftrightarrow\mathscr{B}$ 与 $\mathscr{A}\Rightarrow\mathscr{B}$.

21.5.3 等值演算的几个重要定理

根据已知的等值式,可以推导出另一些等值式,这个过程称作等值演算,现在给出等值演算的几个重要定理. 这些定理的使用是如此频繁,甚至于使用者常常在不自觉的状态下使用了这些定理! 因此,我们把它们特别列出,引起我们的注意!

定理 21.5.8 若 $\mathscr{A}$ 和 $\mathscr{A}\rightarrow\mathscr{B}$ 是永真式,则 $\mathscr{B}$ 必为永真式.

本定理中所说的永真式是$(\mathscr{A}\rightarrow\mathscr{B})$,为了简便,我们常常省去表达式最外层的括号,简洁地记作 $\mathscr{A}\rightarrow\mathscr{B}$. 此约定也适用于其他表达式.

定理 21.5.9 代入定理(substitution) 设 $\mathscr{A}$ 为真值函数, $x_1,x_2,\cdots,x_n$ 是 $\mathscr{A}$ 中出现的命题变量,$\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_n$ 是任意的真值函数. 对于出现在 $\mathscr{A}$ 中的 x_i,用 $\mathscr{A}_i$ 代入,得到

$$\mathscr{A}_{x_1\cdots x_n}^{\mathscr{A}_1\cdots\mathscr{A}_n},$$

若 $\mathscr{A}$ 是永真式,则

$$\mathscr{A}_{x_1\cdots x_n}^{\mathscr{A}_1\cdots\mathscr{A}_n}$$

也是永真式.

例 21.5.10 对于任意的真值函数 $\mathscr{A},\mathscr{B}$,证明:

$$\neg(\mathscr{A}\vee\mathscr{B})\Leftrightarrow(\neg\mathscr{A})\wedge(\neg\mathscr{B}).$$

由真值表可知,对于任意的命题变量 p,q 成立:

$$\neg(p\wedge q)\Leftrightarrow(\neg p)\vee(\neg q),$$

再由定理 21.5.9 即知.

例 21.5.11 对于任意的真值函数 $\mathscr{A},\mathscr{B}$ 证明：

$$(\mathscr{A}\to\mathscr{B})\to(\neg\mathscr{B}\to\neg\mathscr{A})$$

是永真式. 首先由真值表证明 $(P\to Q)\to(\neg Q\to\neg P)$ 是永真式，再利用代入定理.

注意 “代入”运算(或“代入”操作)是人们极为常用的运算，它是一种最简单的操作，人们在使用这种操作时，有时达到了不能自察的地步，甚至对这种简单的操作，究竟要遵守些什么规则，也不明不白. 代入定理就是一个明确提出的规则之一，它告诉我们在执行“代入”操作时要遵守哪些规则，“代入”操作的含义又是什么：

(1) “代入”运算的对象是命题形式(或真值函数)中的某些命题变量(这些命题变量可以在该命题形式中多次出现)，可以用任意的命题形式去“调换”这些命题变量. 当这些变量多次地在原来命题形式中出现时，就必须“处处”进行同样的“调换”(不允许只对一部分命题变量进行“调换”).

(2) 对命题变量作“代入”的命题形式(或真值函数)是任意的.

(3) “代入”运算只能对命题形式中的命题变量进行，不能对它的子公式(不包括由单个命题变量构成的平凡子公式)进行.

(4) “代入”运算的含义是把命题形式中的命题变量看作是新的命题形式，对命题形式进一步地“参数化”(或“泛函化”).

定理 21.5.12 替换定理(replacement) 设 $\mathscr{A}_1$ 是 $\mathscr{A}$ 的子公式，$\mathscr{B}_1$ 是任意的命题形式，在 $\mathscr{A}$ 中出现 $\mathscr{A}_1$ 处(可能不止一处)的用 $\mathscr{B}_1$ 替换 $\mathscr{A}_1$ 后得到命题公式 $\mathscr{B}$. 若 $\mathscr{A}_1\Leftrightarrow\mathscr{B}_1$，则 $\mathscr{A}\Leftrightarrow\mathscr{B}$.

注意 “替换”运算(或“替换”操作)是人们经常使用的运算，它与“等价替换”同义，“替换”定理表达了“替换”操作的条件：

(1) “替换”定理表明，人们可以对命题形式中任何等价的子

公式进行“调换”.

(2) 在进行“替换”操作时,没有必要对原命题形式中出现的同样子公式“处处”调换.

(3) 对命题形式中的命题变量(即特殊的子公式)进行“替换”运算时,就相当于对命题变量“换名”.(对命题变量“换名”时,应遵守的规则是对不同的变量换成不同的“名”.)

下面给出一类特殊的命题形式.

定义 21.5.13 若在命题形式中只出现{$\neg$,$\wedge$,$\vee$}中的联结词,则称它是**受限命题形式**(restricted proposition form).

定义 21.5.14 设有受限命题形式 $\mathscr{A}$ 与 $\mathscr{A}^*$,而 $\mathscr{A}^*$ 是由在命题形式 $\mathscr{A}$ 中进行如下的置换得到的:

(1) 联结词$\wedge$,$\vee$互相置换.

(2) 真假值$\top$,$\bot$互相置换.

则称 $\mathscr{A}^*$ 是 $\mathscr{A}$ 的**对偶式**(dual),或称 $\mathscr{A}$,$\mathscr{A}^*$ **互相对偶**. 也称联结词$\vee$,$\wedge$**互相对偶**.

例 21.5.15 给出下列命题形式(真值函数)的对偶式(对偶真值函数):

(1) $(P\vee Q)\wedge R$.

(2) $(P\wedge Q)\vee\bot$.

(3) $\neg(P\wedge Q)\vee(P\wedge\neg(Q\vee\neg S))$.

根据定义 21.5.14,它们的对偶式分别如下:

(1)* $(P\wedge Q)\vee R$.

(2)* $(P\vee Q)\wedge\top$.

(3)* $\neg(P\vee Q)\wedge(P\vee\neg(Q\wedge\neg S))$.

下面的定理 21.5.16 表明了真值函数及其对偶式之间的紧密联系.

定理 21.5.16 **对偶原理**(dual principle) 设命题形式 $\mathscr{A}(x_1,\cdots,x_n)$与命题形式 $\mathscr{A}^*(x_1,\cdots,x_n)$互为对偶(其中 $x_1,\cdots,x_n$

是原子命题变量),则有:

(1) $\neg \mathscr{A}(x_1, x_2, \cdots, x_n) \Leftrightarrow \mathscr{A}^*(\neg x_1, \neg x_2, \cdots, \neg x_n)$.

(2) $\mathscr{A}(\neg x_1, \neg x_2, \cdots, \neg x_n) \Leftrightarrow \neg \mathscr{A}^*(x_1, x_2, \cdots, x_n)$.

(注意定义 21.5.16 中的结论(1),(2)是可以相互推导的.)

例 21.5.17 设命题形式是 $\mathscr{A}(p,q,r) = \neg p \wedge \neg(q \vee r)$. 验证对偶原理.

由定义 21.5.14,有

$$\mathscr{A}^*(p,q,r) = \neg p \vee \neg(q \wedge r),$$

所以

$$\begin{aligned}
\mathscr{A}^*(\neg p, \neg q, \neg r) &= \neg(\neg p) \vee \neg((\neg q) \wedge (\neg r)) \\
&\Leftrightarrow p \vee (\neg\neg q \vee \neg\neg r) \\
&\Leftrightarrow p \vee q \vee r. \\
\mathscr{A}(\neg p, \neg q, \neg r) &= (\neg\neg p) \wedge \neg(\neg q \vee \neg r) \\
&\Leftrightarrow p \wedge (\neg\neg q \wedge \neg\neg r) \\
&\Leftrightarrow p \wedge q \wedge r. \\
\neg \mathscr{A}^*(p,q,r) &\Leftrightarrow \neg(\neg p \vee \neg(q \wedge r)) \\
&\Leftrightarrow \neg\neg p \wedge \neg\neg(q \wedge r) \\
&\Leftrightarrow p \wedge q \wedge r.
\end{aligned}$$

所以

$$\neg \mathscr{A}(p,q,r) \Leftrightarrow \mathscr{A}^*(\neg p, \neg q, \neg r)$$

$$\mathscr{A}(\neg p, \neg q, \neg r) \Leftrightarrow \neg \mathscr{A}^*(p,q,r).$$

定理 21.5.18 设命题形式 $\mathscr{A}, \mathscr{A}^*$ 互为对偶;$\mathscr{B}, \mathscr{B}^*$ 也互为对偶,则当 $\mathscr{A} \Leftrightarrow \mathscr{B}$ 时,有:

(1) $\mathscr{A}^* \Leftrightarrow \mathscr{B}^*$.

(2) $(\mathscr{A}^*)^* \Leftrightarrow \mathscr{A}$.

定理 21.5.18 中的 $(\mathscr{A}^*)^*$ 常记作 $\mathscr{A}^{**}$.

注 (1) 由于有对偶原理,则可以理解许多等值变换的规律总是成"对"出现的. 实际上每"对"中间两个等价公式是互为对

偶的.

(2) 由于在命题逻辑中有对偶原理,故可以很方便地从一个定理得出另一个定理. 同时可以把寻找对偶式的操作看成是一种运算.

(3) 在对偶运算中,只对真假值$\top$,$\bot$相互置换,对联结词$\vee$,$\wedge$相互置换,而对于否定词,保留不变.

(4) 利用对偶原理可以从命题形式$\mathscr{A}$找到它的否定式$\neg\mathscr{A}$. 只要把$\mathscr{A}$换成它的对偶式$\mathscr{A}^*$,再把出现于$\mathscr{A}$中的所有原子变量换成它的否定式即可.

21.5.4 等值演算中常用的命题等值式与重言式

以下是常用的等值式与重言式.

公式 21.5.19 常用等值式(useful equivelant):

(1) $\neg\neg\mathscr{A}\Leftrightarrow\mathscr{A}$. (双重否定律)

(2) $\mathscr{A}\wedge\mathscr{B}\Leftrightarrow\mathscr{B}\wedge\mathscr{A}$. (交换律)

$\mathscr{A}\vee\mathscr{B}\Leftrightarrow\mathscr{B}\vee\mathscr{A}$.

(3) $(\mathscr{A}\wedge\mathscr{B})\wedge\mathscr{C}\Leftrightarrow\mathscr{A}\wedge(\mathscr{B}\wedge\mathscr{C})$. (结合律)

$(\mathscr{A}\vee\mathscr{B})\vee\mathscr{C}\Leftrightarrow\mathscr{A}\vee(\mathscr{B}\vee\mathscr{C})$.

(4) $\mathscr{A}\wedge(\mathscr{B}\vee\mathscr{C})\Leftrightarrow(\mathscr{A}\wedge\mathscr{B})\vee(\mathscr{A}\wedge\mathscr{C})$. (分配律)

$\mathscr{A}\vee(\mathscr{B}\wedge\mathscr{C})\Leftrightarrow(\mathscr{A}\vee\mathscr{B})\wedge(\mathscr{A}\vee\mathscr{C})$.

(5) $\neg(\mathscr{A}\wedge\mathscr{B})\Leftrightarrow(\neg\mathscr{A})\vee(\neg\mathscr{B})$. (DeMorgan 律)

$\neg(\mathscr{A}\vee\mathscr{B})\Leftrightarrow(\neg\mathscr{A})\wedge(\neg\mathscr{B})$.

(6) $\mathscr{A}\vee\mathscr{A}\Leftrightarrow\mathscr{A}$. (恒等律)

$\mathscr{A}\wedge\mathscr{A}\Leftrightarrow\mathscr{A}$.

(7) $\mathscr{A}\wedge(\mathscr{B}\vee\neg\mathscr{B})\Leftrightarrow\mathscr{A}$.

$\mathscr{A}\vee(\mathscr{B}\wedge\neg\mathscr{B})\Leftrightarrow\mathscr{A}$.

(8) $\mathscr{A}\vee(\mathscr{B}\vee\neg\mathscr{B})\Leftrightarrow\top$.

$\mathscr{A}\wedge(\mathscr{B}\wedge\neg\mathscr{B})\Leftrightarrow\bot$.

(9) $\mathscr{A}\to\mathscr{B}\Leftrightarrow\neg\mathscr{B}\to\neg\mathscr{A}$. (逆否律)

(10) $\mathscr{A}\to\mathscr{B}\Leftrightarrow\neg\mathscr{A}\vee\mathscr{B}$.

(11) $\neg(\mathscr{A}\to\mathscr{B})\Leftrightarrow\mathscr{A}\wedge\neg\mathscr{B}$.

(12) $\mathscr{A}\to(\mathscr{B}\to\mathscr{C})\Leftrightarrow(\mathscr{A}\wedge\mathscr{B})\to\mathscr{C}$.

(13) $\mathscr{A}\leftrightarrow\mathscr{B}\Leftrightarrow(\mathscr{A}\to\mathscr{B})\wedge(\mathscr{B}\to\mathscr{A})$.

(14) $\mathscr{A}\leftrightarrow\mathscr{B}\Leftrightarrow(\mathscr{A}\wedge\mathscr{B})\vee(\neg\mathscr{A}\wedge\neg\mathscr{B})$.

(15) $\neg(\mathscr{A}\leftrightarrow\mathscr{B})\Leftrightarrow\mathscr{A}\leftrightarrow\mathscr{B}$.

从上述众多的等值式(等价式)可以看到,真值函数的表达式不是唯一的. 经验表明,自觉地使用逻辑规律与不自觉地使用逻辑规律是完全不一样的. 熟悉这些规律可使人们的思维正确而敏锐.

公式 21.5.20 常用永真(重言)蕴含式:

(1) $\mathscr{A}\wedge\mathscr{B}\Rightarrow\mathscr{A}$, (简化规则/simplication)

$\mathscr{A}\wedge\mathscr{B}\Rightarrow\mathscr{B}$.

(2) $\mathscr{A}\Rightarrow\mathscr{A}\vee\mathscr{B}$, (添加规则/addition)

$\mathscr{B}\Rightarrow\mathscr{A}\vee\mathscr{B}$.

(3) $\neg\mathscr{A}\Rightarrow\mathscr{A}\to\mathscr{B}$,

$\mathscr{B}\Rightarrow\mathscr{A}\to\mathscr{B}$.

(4) $\neg(\mathscr{A}\to\mathscr{B})\Rightarrow\mathscr{A}$,

$\neg(\mathscr{A}\to\mathscr{B})\Rightarrow\neg\mathscr{B}$.

(5) $\mathscr{A},\mathscr{B}\Rightarrow\mathscr{A}\wedge\mathscr{B}$.

(6) $\mathscr{A},\mathscr{A}\to\mathscr{B}\Rightarrow\mathscr{B}$. (分离规则/modus ponens)

(7) $\neg\mathscr{A},\mathscr{A}\vee\mathscr{B}\Rightarrow\mathscr{B}$. (选言三段论/disjuntive syllogism)

(8) $\neg\mathscr{B},\mathscr{A}\to\mathscr{B}\Rightarrow\neg\mathscr{A}$. (否定后件式/modus tollens)

(9) $\mathscr{A}\to\mathscr{B},\mathscr{B}\to\mathscr{C}\Rightarrow\mathscr{A}\to\mathscr{C}$.

(假言三段论/hypothelical syllogism)

(10) $\mathscr{A}\vee\mathscr{B},\mathscr{A}\to\mathscr{C},\mathscr{B}\to\mathscr{C}\Rightarrow\mathscr{C}$. (二难推理/dilemma)

21.6 范式与真值表技术

命题逻辑中的命题形式是多种多样的，如何判断它们是重言式，矛盾式还是可满足公式？通常可通过命题形式的真值表或等值演算获知. 但是对于大量的命题形式，用计算机进行处理，要求把命题形式表达成一种规范的形式，这就是命题形式的范式问题.

由于联结词集合$\{\neg,\wedge,\vee\}$是完备的(完全的)，我们有下述定理.

定理 21.6.1 任意命题形式必存在与之等值的受限命题形式.

受限命题形式中的某种规范形式，称为范式.

定义 21.6.2 (1) 由原子命题变量或原子命题变量的否定式构成的合取式称为**初等积**(elementary product). (2) 由原子命题变量或原子命题变量的否定式构成的析取式称为**初等和**(elementary sum).

例 21.6.3 设 P,Q 为任意的原子命题，则 $P,\neg P,\neg P\wedge Q$, $\neg Q\wedge P\wedge\neg P, P\wedge\neg P, Q\wedge\neg P$ 都是初等积，而 $P,\neg P\vee Q$, $\neg Q\vee P\vee\neg P, P\vee\neg P, Q\vee\neg P$ 都是初等和.

初等和或初等积的部分表达式，如果仍旧是初等和或初等积时，则称它们是原给初等和或初等积的**因子**(factor). 例如，初等积$\neg Q\wedge P\wedge\neg P$ 的因子有：$\neg Q, P, P\wedge\neg P, \neg P, \neg Q\wedge P$, $\neg Q\wedge P\wedge\neg P$ 等.

关于初等和与初等积，有以下性质.

定理 21.6.4 一个初等积是永假的充要条件是，它至少含有一对永假因子. 一个初等和是永真的充要条件是，它至少含有一对永真因子.

定义 21.6.5 (1) 初等积的析取式称为**析取范式**(disjunctive

normal form). (2) 初等和的合取式称为**合取范式**(conjunctive normal form).

极取范式或合取范式统称范式.

定理 21.6.6 范式存在定理 任意命题形式(真值函数)必存在与之等值的范式.

例 21.6.7 寻找下列命题形式的析取范式:

(1) $P\wedge(P\rightarrow Q)$;

(2) $\neg(P\vee Q)\leftrightarrow(P\wedge Q)$.

解

(1) $P\wedge(P\rightarrow Q)$

$\Leftrightarrow P\wedge(\neg P\vee Q)$ (公式 21.5.19(10))

$\Leftrightarrow(P\wedge\neg P)\vee(P\wedge Q)$. (公式 21.5.19(4))

(2) $\neg(P\rightarrow Q)\leftrightarrow(P\wedge Q)$

$\Leftrightarrow(\neg(P\rightarrow Q)\wedge(P\wedge Q))\vee(\neg(\neg(P\rightarrow Q))\wedge\neg(P\wedge Q))$ (公式 21.5.19(14))

$\Leftrightarrow(\neg(P\rightarrow Q)\wedge(P\wedge Q))\vee((P\rightarrow Q)\wedge\neg(P\wedge Q))$ (公式 21.5.19(1))

$\Leftrightarrow(\neg(\neg P\vee Q)\wedge(P\wedge Q))\vee((\neg P\vee Q)\wedge\neg(P\wedge Q))$ (公式 21.5.19(10))

$\Leftrightarrow((P\wedge\neg Q)\wedge(P\wedge Q))\vee((\neg P\vee Q)\wedge(\neg P\vee\neg Q))$ (公式 21.5.19(5))

$\Leftrightarrow(P\wedge\neg Q\wedge P\wedge Q)\vee(\neg P\wedge\neg P)\vee(\neg P\wedge\neg Q)\vee(Q\wedge\neg P)\vee(Q\wedge\neg Q)$ (公式 21.5.19(4))

$\Leftrightarrow(P\wedge\neg Q\wedge Q)\vee(\neg P)\vee(\neg P\wedge\neg Q)\vee(Q\wedge\neg P)\vee(Q\wedge\neg Q)$ (公式 21.5.19(6))

$\Leftrightarrow\perp\vee\neg P\vee(\neg P\wedge\neg Q)\vee(Q\wedge\neg P)\vee\perp$

$\Leftrightarrow\neg P\vee(\neg P\wedge\neg Q)\vee(Q\wedge\neg P)$

$\Leftrightarrow\neg P\vee(Q\wedge\neg P)$

$\Leftrightarrow\neg P$.

从例 21.6.7(2)可以看出 $\neg P\vee(\neg P\wedge\neg Q)\vee(Q\wedge\neg P)$，$\neg P\vee(Q\wedge\neg P)$以及$\neg P$都是命题形式(2)的范式. 真值函数的范式不是唯一的，并且通过析取范式可以看到，如果已给真值函数的析取范式中的每一个初等积为永假式，那么该真值函数一定是永假函数.

现在给出实现定理 21.6.6 的算法.

算法 21.6.8　判诀过程(decision procedure)

算法的步骤如下：

(1) 应用蕴含律或双蕴含律消去条件式或双条件式$\rightarrow$，$\leftrightarrow$.

(1.1) $\mathscr{A}\leftrightarrow\mathscr{B}\Leftrightarrow(\mathscr{A}\rightarrow\mathscr{B})\wedge(\mathscr{B}\rightarrow\mathscr{A})$.

(1.2) $\mathscr{A}\rightarrow\mathscr{B}\Leftrightarrow\neg\mathscr{A}\vee\mathscr{B}$.

(2) 重复使用双重否定律与 DeMorgan 律，把否定词“深入”作用于原子命题变元.

(2.1) $\neg(\neg\mathscr{A})\Leftrightarrow\neg\neg\mathscr{A}\Leftrightarrow\mathscr{A}$.

(2.2) $\neg(\mathscr{A}\vee\mathscr{B})\Leftrightarrow\neg\mathscr{A}\wedge\neg\mathscr{B}$.

(2.3) $\neg(\mathscr{A}\wedge\mathscr{B})\Leftrightarrow\neg\mathscr{A}\vee\neg\mathscr{B}$.

(3) 重复使用分配律.

(3.1) $\mathscr{A}\vee(\mathscr{B}\wedge\mathscr{C})\Leftrightarrow(\mathscr{A}\vee\mathscr{B})\wedge(\mathscr{A}\vee\mathscr{C})$.

(3.2) $\mathscr{A}\wedge(\mathscr{B}\vee\mathscr{C})\Leftrightarrow(\mathscr{A}\wedge\mathscr{B})\vee(\mathscr{A}\wedge\mathscr{C})$.

例 21.6.9　使用算法 21.6.8 寻找下列真值函数的析取范式：

(1) $(P\vee\neg Q)\rightarrow R$.

(2) $(P\wedge(Q\rightarrow R))\rightarrow S$.

解　(1) $(P\vee\neg Q)\rightarrow R$

$\Leftrightarrow\neg(P\vee\neg Q)\vee R$　　(1.2)

$\Leftrightarrow(\neg P\wedge\neg\neg Q)\vee R$　　(2.2)

$\Leftrightarrow(\neg P\wedge Q)\vee R$.　　(2.1)

上式即为所求的析取范式.

(2) $(P\wedge(Q\rightarrow R))\rightarrow S$

$\Leftrightarrow(P\wedge(\neg Q\vee R))\rightarrow S$　　(1.2)

$\Leftrightarrow (P \wedge (\neg Q \vee R)) \vee S$ (1.2)

$\Leftrightarrow \neg (P \vee \neg (\neg Q \vee R)) \vee S$ (2.3)

$\Leftrightarrow \neg P \vee (\neg \neg Q \wedge \neg R) \vee S$ (2.2)

$\Leftrightarrow \neg P \vee (Q \wedge \neg R) \vee S$ (2.1)

$\Leftrightarrow (\neg P) \vee (Q \wedge \neg R) \vee S.$

上式即为所求的析取范式.

例 21.6.10 使用算法 21.6.8 求下列真值函数的合取范式.

(1) $P \wedge (P \rightarrow Q)$.

(2) $\neg (P \vee Q) \leftrightarrow (P \wedge Q)$.

解 (1) $P \wedge (P \rightarrow Q) \Leftrightarrow P \wedge (\neg P \vee Q)$. (1.2)

(2) $\neg (P \vee Q) \leftrightarrow (P \wedge Q)$

$\Leftrightarrow (\neg (P \vee Q) \rightarrow (P \wedge Q)) \wedge ((P \wedge Q) \rightarrow \neg (P \vee Q))$ (1.1)

$\Leftrightarrow (\neg \neg (P \vee Q) \vee (P \wedge Q)) \wedge (\neg (P \wedge Q) \vee \neg (P \vee Q))$

(1.2)

$\Leftrightarrow ((P \vee Q) \vee (P \wedge Q)) \wedge (\neg (P \wedge Q) \vee (\neg P \wedge \neg Q))$

(2.1),(2.2),(2.3)

$\Leftrightarrow ((P \vee Q \vee P) \wedge (P \vee Q \vee Q)) \wedge ((\neg (P \wedge Q) \vee \neg P) \wedge$
$(\neg (P \wedge Q) \vee \neg Q))$ (3.1),(3.2)

$\Leftrightarrow ((P \vee Q \vee P) \wedge (P \vee Q \vee Q)) \wedge ((\neg P \vee \neg Q \vee \neg P) \wedge$
$(\neg P \vee \neg Q \vee \neg Q))$ (2.2),(2.3)

$\Leftrightarrow (P \vee Q \vee P) \wedge (P \vee Q \vee Q) \wedge (\neg P \vee \neg Q \vee \neg P) \wedge$
$(\neg P \vee \neg Q \vee \neg Q).$

注 (1) 与析取范式一样,一个命题形式的合取范式,也不是唯一的.

(2) 如果已给命题函数的合取范式中的每一个初等和均为永真式,则该命题形式就是永真函数.

(3) 如果已给命题函数的析取范式中的每一个初等积均为永假式,那么该命题形式就是永假函数.

因此，利用析取范式，可以较方便地判断一个真值函数是否永假，利用合取范式，可以较方便地判断一个真值函数是否永真.

命题形式的规范形式—范式，虽然限制了表达式中的联结词，但由于同一个真值函数可以有许多不同的范式，因此还不能利用计算机进行统一处理. 还必须对范式作进一步地限制，这就产生了正则范式的问题.

定义 21.6.11 形如 $\bigvee_{i=1}^{k}(\bigwedge_{j=1}^{n} Q_{ij})$ 的真值函数，称为**正则析取范式**(disjunctive normal form)，其中 Q_{ij} 是原子命题变元或者是原子命题变元的否定式.

注 正则析取范式中的 $\bigwedge_{j=1}^{n} Q_{ij}$ 详细写出就是：$\bigwedge_{j=1}^{n} Q_{ij} = Q_{i1} \wedge Q_{i2} \wedge \cdots \wedge Q_{in}$，其中 Q_{ij} 是原子命题变元或者是原子命题变元的否定式，上述表达式中非永假的合取式(即在 $Q_{i1},\cdots,Q_{in}$ 中不出现互为否定的原子命题变元，例如 $Q_{i1} = \neg Q_{i3}$)，称作**极小项**(mini term).

例 21.6.12 设 p,q 为两个命题变元，它可以组成的极小项为：

$$p \wedge q, p \wedge \neg q, \neg p \wedge q, \neg p \wedge \neg q.$$

由此可知，正则析取范式是由极小项通过析取运算所构成的.

还有另一种范式.

定义 21.6.13 形如 $\bigwedge_{i=1}^{k}(\bigvee_{j=1}^{n} Q_{ij})$ 的真值函数，称为**正则合取范式**(conjunctive normal form)，其中 Q_{ij} 是原子命题变元或者是原子命题变元的否定式.

注 正则合取范式中 $\bigvee_{j=1}^{n} Q_{ij}$ 就是

$$\bigvee_{j=1}^{n} Q_{ij} = Q_{i1} \vee Q_{i2} \vee \cdots \vee Q_{in},$$

其中非永真的析取式(即在 $Q_{i1},\cdots,Q_{in}$ 中不出现互为否定的原子

命题变元，例如 $Q_{i1}=\neg Q_{i3}$），称为**极大项**(max term).

例 21.6.14 设 p,q 为两个命题变元，它可以组成的极大项为

$$p\vee q, p\vee \neg q, \neg p\vee q, \neg p\vee \neg q.$$

由此可知，正则合取范式是由极大项通过合取运算构成的.

正则析取范式与正则合取范式统称**正则范式**，它们有下述重要的性质.

定理 21.6.15 正则范式存在定理 命题逻辑中的任意命题形式，都有与之等值的正则范式. 这种范式是唯一的.

推论 21.6.16 (1) 每个非永假的命题形式必逻辑等值于某个正则析取范式.

(2) 每个非永真的命题形式必逻辑等值于某个正则合取范式.

从真值函数的范式出发，执行下述算法可以得到正则范式.

算法 21.6.17 算法的步骤如下：

(1) 添加 把缺少某一个命题变元(例如 p)的合(析)取式 $\mathscr{A}$，替换成含有该变元 p 的等值式，

(1.1) $\mathscr{A}\Leftrightarrow\mathscr{A}\wedge(p\vee\neg p)$，

或 (1.2) $\mathscr{A}\Leftrightarrow\mathscr{A}\vee(p\wedge\neg p)$.

(2) 消去 删去重复出现的极小项或极大项.

(3) 排序 把极小项或极大项按线性序或字典序排序.

例 21.6.18 找出命题形式 $(P\vee\neg Q)\rightarrow R$ 的正则析取范式.

解 首先使用算法 21.6.8 找出命题形式 $(P\vee\neg Q)\rightarrow R$ 的析取范式：

$$(P\vee\neg Q)\rightarrow\Leftrightarrow(\neg P\wedge Q)\vee R.$$

再利用算法 21.6.17 找出析取范式

$$(\neg P\wedge Q)\vee R$$

的正则析取范式.

首先注意范式中命题变元有 3 个，即 P,Q,R，所以它们的极小项中的命题原子变元也是 P,Q,R.

由于

$$(\neg P \wedge Q) \Leftrightarrow (\neg P \wedge Q \wedge (R \vee \neg R)) \quad (1.1)$$
$$\Leftrightarrow (\neg P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R),$$

$$R \Leftrightarrow (R \wedge (Q \vee \neg Q) \wedge (P \vee \neg P)) \quad (1.1)$$
$$\Leftrightarrow R \wedge ((Q \wedge P) \vee (Q \wedge \neg P) \vee (\neg Q \wedge P) \vee (\neg Q \wedge \neg P))$$
$$\Leftrightarrow (R \wedge Q \wedge P) \vee (R \wedge Q \wedge \neg P) \vee (R \wedge \neg Q \wedge P) \vee (R \wedge \neg Q \wedge \neg P),$$

所以

$$(\neg P \wedge Q) \vee R \Leftrightarrow (\neg P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (R \wedge Q \wedge P) \vee$$
$$\vee (R \wedge Q \wedge \neg P) \vee (R \wedge \neg Q \wedge P) \vee (R \wedge \neg Q \wedge \neg P)$$
$$\Leftrightarrow (\neg P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (R \wedge Q \wedge P) \vee$$
$$\vee (R \wedge \neg Q \wedge P) \vee (R \wedge \neg Q \wedge \neg P) \quad (2)$$
$$\Leftrightarrow (P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee$$
$$\vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R). \quad (3)$$

例 21.6.19 找出下述命题形式的正则合取范式

$$(P \wedge (Q \rightarrow R)) \rightarrow S.$$

首先求出上式的合取范式

$$(P \wedge (Q \rightarrow R)) \rightarrow S \Leftrightarrow (S \vee \neg P \vee Q) \wedge (S \vee \neg P \vee \neg R).$$

现在利用算法 21.6.17 寻找它的正则合取范式：

由于原命题含有 4 个原子命题：P,Q,R,S，故它的极大项中也含有 4 个原子命题. 所以

$$(S \vee \neg P \vee Q) \wedge (S \vee \neg P \vee \neg R)$$
$$\Leftrightarrow (S \vee \neg P \vee Q \vee (R \wedge \neg R)) \wedge (S \vee \neg P \vee \neg R \vee (Q \wedge \neg Q)) \quad (1)$$
$$\Leftrightarrow (S \vee \neg P \vee Q \vee R) \wedge (S \vee \neg P \vee Q \vee \neg R) \wedge$$

$$(S\vee\neg P\vee\neg R\vee Q)\wedge(S\vee\neg P\vee\neg R\vee\neg Q)$$

$$\Leftrightarrow(\neg P\vee Q\vee R\vee S)\wedge(\neg P\vee Q\vee\neg R\vee S)\wedge(\neg P\vee\neg Q\vee\neg R\vee S).\qquad (2),(3)$$

上式即为所求的正则合取范式.

以上介绍了对任意的命题形式寻找与之等值的范式或正则范式的算法. 现在再给出一种由真值函数的真值表找到其正则范式的算法,称为**真值表技术**(technique of truth table). 先看下例.

例 21.6.20 已给真值函数: $P\to(Q\to R)$,求出它的正则析取范式.

解 首先列出真值表 21.12.

表 21.12

P	Q	R	$Q\to R$	$P\to(Q\to R)$	注释
$\top$	$\top$	$\top$	$\top$	$\top$	←
$\top$	$\top$	$\bot$	$\bot$	$\bot$	
$\top$	$\bot$	$\top$	$\top$	$\top$	←
$\top$	$\bot$	$\bot$	$\top$	$\top$	←
$\bot$	$\top$	$\top$	$\top$	$\top$	←
$\bot$	$\top$	$\bot$	$\bot$	$\top$	←
$\bot$	$\bot$	$\top$	$\top$	$\top$	←
$\bot$	$\bot$	$\bot$	$\top$	$\top$	←

现在给出由真值表构造出正则析取范式的算法,按下列步骤执行:

(1) 选出已给函数取得$\top$值所在行对应的变元值(在表 21.12 中这种行的右端用箭头←标示出来)如下:

1) $\top\ \top\ \top$,

3) $\top\ \bot\ \top$,

4) $\top\ \bot\ \bot$,

5）$\perp \top \top$，

6）$\perp \top \perp$，

7）$\perp \perp \top$，

8）$\perp \perp \perp$.

（2）把上面选出的各行变元值“还原”成相应的原子命题符号，值为$\top$者“还原”为原变量，值为$\perp$者“还原”成原变量的否定式：

1′）$P\,Q\,R$，

3′）$P\neg Q\,R$，

4′）$P\,Q\neg R$，

5′）$\neg P\,Q\,R$，

6′）$\neg P\,Q\ \neg R$，

7′）$\neg P\neg Q\,R$，

8′）$\neg P\neg Q\neg R$.

（3）将上述各行变量分别构成合取式：

1″）$P\wedge Q\wedge R$，

3″）$P\wedge\neg Q\wedge R$，

4″）$P\wedge\neg Q\wedge\neg R$，

5″）$\neg P\wedge Q\wedge R$，

6″）$\neg P\wedge Q\wedge\neg R$，

7″）$\neg P\wedge\neg Q\wedge R$，

8″）$\neg P\wedge\neg Q\wedge\neg R$.

上述 1″），3″），…，8″）均为原真值函数的极小项.

（4）把上述极小项用析取词联结，即得所求正则析取范式：

$$P\to(Q\to R)\Leftrightarrow(P\wedge Q\wedge R)\vee(P\wedge\neg Q\wedge R)\vee(P\wedge\neg Q\wedge\neg R)\vee(\neg P\wedge Q\wedge R)\vee(\neg P\wedge Q\wedge\neg R)\vee(\neg P\wedge\neg Q\wedge R)\vee(\neg P\wedge\neg Q\wedge\neg R).$$

应用真值表技术，无需事先知道真值函数$\mathscr{F}$的任何表达式，只要知道给定的真值表就行了. 因此对于包含大量命题变量的复杂命题形式(尤其在工程技术的应用中)找到$\mathscr{F}$的正则范式是极为重要的. 见下面的例.

例 21.6.21 求出由真值表 21.13 给出的真值函数$\mathscr{F}$的正则范式.

表 21.13

P	Q	R	$\mathscr{F}$	注释
$\top$	$\top$	$\top$	$\top$	←
$\top$	$\top$	$\bot$	$\bot$	
$\top$	$\bot$	$\top$	$\top$	←
$\top$	$\bot$	$\bot$	$\bot$	
$\bot$	$\top$	$\top$	$\top$	←
$\bot$	$\top$	$\bot$	$\top$	←
$\bot$	$\bot$	$\top$	$\bot$	
$\bot$	$\bot$	$\bot$	$\bot$	

解 依照例 21.6.20 中所使用的真值表技术，函数$\mathscr{F}$的正则析取范式为

$$\mathscr{F} \Leftrightarrow (P \wedge Q \wedge K) \vee (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R).$$

显然，当$\mathscr{F}$取值为$\bot$时，$\neg \mathscr{F}$取值为$\top$，于是$\neg \mathscr{F}$的正则析取范式是

$$\neg \mathscr{F} \Leftrightarrow (P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R).$$

从而由双重否定律及 DeMorgan 律，有

$$\mathscr{F} \Leftrightarrow \neg \neg \mathscr{F} \Leftrightarrow (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee Q \vee \neg R) \wedge (P \vee Q \vee R).$$

上式就是$\mathscr{F}$的正则合取范式.

由上例可知,对任意的真值函数$\mathscr{A}$而言,$\neg\mathscr{A}$的正则析取范式就是$\mathscr{A}$的正则合取范式;反之,$\neg\mathscr{A}$的正则合取范式就是$\mathscr{A}$的正则析取范式.所以对任何真值函数而言,知道它的一种正则范式就足够了.

21.7 命题逻辑的推理系统 命题演算

对于命题逻辑中的命题形式(真值函数),判断它是永真式、矛盾式或可满足式,基本只有两类方法.一类是所谓的"语义"方法,就是对于真值函数进行赋值,对原子命题变量赋值(即"真","假"值)后,计算真值函数的"值".本质上,就是真值表表示法.另一类就是建立(形式)推理系统.粗略地说,就是从少量的公理(永真函数)与推理规则出发,对复杂的命题形式进行"证明"或"反驳".这就是所谓的"语法"方法.正由于此,有些文献中,也称命题演算为命题逻辑语言.

命题逻辑的推理也可以分成自然推理和公理系统推理两类.在自然推理系统中强调推理规则(或推理模式),进行推理时可以从任意的前提出发,证明系统中的定理.在公理系统推理系统中,强调公理.进行推理时必须从公理出发,应用推理规则证明系统中的定理.

21.7.1 公理系统 L

公理系统,就是从事先给定的公理出发,根据推理规则推导出一系列的定理.例如,欧氏几何学就是一个古典的公理系统.由命题逻辑中的重言式组成的命题演算就是一个现代的公理系统.

现在给出命题逻辑的公理系统L.

定义 21.7.1 公理系统L定义如下:

(1) 符号(字母)库:

命题字母(statement letter): $P,Q,R,\cdots,P_1,Q_1,R_1,\cdots,P_2,Q_2,R_2,\cdots$.

初始联结词(primitive connective): $\neg,\rightarrow$

辅助符号(auxiliary symbol): 括号),(.

(2) 合式公式集(公式集)

1) 所有的命题字母都是合式公式.

2) 若 $\mathscr{A},\mathscr{B}$ 是合式公式,则$(\neg\mathscr{A})$,$(\mathscr{A}\rightarrow\mathscr{B})$也是合式公式.

3) 合式公式仅由 1),2)构成.

(3) 公理集(axiom)

用公理模式给出,其中 $\mathscr{A},\mathscr{B},\mathscr{C}$ 是 L 中任意的合式公式.

A1 $(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$.

A2 $((\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))\rightarrow((\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow\mathscr{C})))$.

A3 $(((\neg\mathscr{A})\rightarrow(\neg\mathscr{B}))\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$或

$(((\neg\mathscr{A})\rightarrow(\neg\mathscr{B}))\rightarrow(((\neg\mathscr{A})\rightarrow\mathscr{B})\rightarrow\mathscr{A}))$.

注 为了书写方便,上面的公理及合式公式中的最外层的括号及$(\neg\mathscr{A})$的括号可以省去.

(4) 推理规则集(rule of inference)

从 $\mathscr{A}$ 和 $\mathscr{A}\rightarrow\mathscr{B}$ 可以推演出 $\mathscr{B}$. 这个规则称为 modus ponens,简称 MP 规则. 常说: $\mathscr{B}$ 是 $\mathscr{A}$ 和 $\mathscr{A}\rightarrow\mathscr{B}$ 的**直接推论(直接后承)**(direct consequence). 系统 L 中,仅有这一条推理(推演)规则.

由定义 21.7.1 给出的 L 就是命题逻辑的公理推理系统. 下面再给出 L 中有关推演的重要概念及性质.

定义 21.7.2 (1) 设 Γ 是系统 L 中的公式集,$\mathscr{A}\in L$,若存在 L 中的公式序列 $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_n$,满足以下条件之一:

1) $\mathscr{A}_n=\mathscr{A}$;

2) $\mathscr{A}_i(1\leqslant i\leqslant n)$是 L 中的公理;

或 3) $\mathscr{A}_i\in\Gamma\ (1\leqslant i\leqslant n)$;

或　4) $\mathscr{A}_i(1\leqslant i\leqslant n)$是序列中较前的两个公式应用推理规则 MP 后的直接推论.

则称 $\mathscr{A}$ 是 Γ 的**推论**(后承)(consequence),记作 $\Gamma\vdash_L\mathscr{A}$,简记作 $\Gamma\vdash\mathscr{A}$.

(2) 定义(1)中的序列 $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_n$,称为 $\mathscr{A}$ 从 Γ 的**证明(演绎)**(proof/deduction),Γ 称作证明的**假设**(hypothese)或**前提**(premise).

(3) 若 Γ 是有限集$\{\mathscr{B}_1,\cdots,\mathscr{B}_n\}$,则记号$\{\mathscr{B}_1,\cdots,\mathscr{B}_n\}\vdash\mathscr{A}$简记为 $\mathscr{B}_1,\cdots,\mathscr{B}_n\vdash\mathscr{A}$.

(4) 当 Γ 是空集 $\varnothing$ 时,则记号 $\varnothing\vdash\mathscr{A}$ 简记为 $\vdash\mathscr{A}$,称公式 $\mathscr{A}$ 是 L 中的**定理**(theorem)或**可证公式**(provable formula).

注　关于定义 21.7.2 添加说明如下:

(1) 系统 L 中的 Γ 是任意的公式集,其中的公式可以是 L 中的公理或定理,也可以不是 L 中的公理或定理,换言之,它可以是 L 中若干个任意的公式所构成的集合. 并且 Γ 可以是无限集,也可以是有限集或空集.

(2) 从 Γ 的一个演绎可以看作是这样的一个证明,Γ 中的公式是暂时当作公理来使用的.

(3) 在定义中,仅仅涉及到公式序列的存在性,并不要求它的唯一性.

(4) 本定义给出了 L 中的定理是从公式的空集合可证明的公式(同时 L 中的一个证明就是从 $\varnothing$ 的一个演绎). 这是因为当 $\Gamma=\varnothing$ 时,公式序列 $\mathscr{A}_1,\cdots,\mathscr{A}_n,\mathscr{A}$ 中的任意公式,除了或者是公理,或者是其前面两个公式使用规则 MP 所得的直接推论以外,再也没有任何额外的公式.

(5) 从定义可知公式序列 $\mathscr{A}_1,\cdots,\mathscr{A}_n,\mathscr{A}$ 中的任意公式,要么是公理,要么就是定理.

(6) 符号"$\vdash$"不是系统 L 中的符号,任何出现它的表达式都

不是 L 中的公式. 例如 $\vdash_L \mathscr{A}$ 不是 L 中的公式,而表示关于 L 的一个命题,它是说:公式 $\mathscr{A}$ 是 L 中的一条定理.

(7) 使用的花体字母 $\mathscr{A},\mathscr{B},\mathscr{C}$ 等也不在系统 L 内. 为了方便,采用它们表示 L 中任意的不确指的公式,或用来作关于 L 的一般断定.

下面举出具体的例子,说明在系统 L 中是如何进行推演的.

例 21.7.3 给出 $\{\mathscr{A},(\mathscr{B}\to(\mathscr{A}\to\mathscr{C}))\}\vdash_L(\mathscr{B}\to\mathscr{C})$ 的一个证明.

(1) $\mathscr{A}$, 假设

(2) $\mathscr{B}\to(\mathscr{A}\to\mathscr{C})$, 假设

(3) $\mathscr{A}\to(\mathscr{B}\to\mathscr{A})$, (A1)

(4) $\mathscr{B}\to\mathscr{A}$, (1)(3)MP

(5) $(\mathscr{B}\to(\mathscr{A}\to\mathscr{C}))\to((\mathscr{B}\to\mathscr{A})\to(\mathscr{B}\to\mathscr{C}))$, (A2)

(6) $(\mathscr{B}\to\mathscr{A})\to(\mathscr{B}\to\mathscr{C})$, (2)(5)MP

(7) $\mathscr{B}\to\mathscr{C}$. (4)(6)MP

注 对于例题 21.7.3,如果把前提作为"树叶"(leaf),把公式作为"结点"(node),把变换作为"弧"(arc). 则可以把上面的推导过程用一棵"证明树"表示出来(见图 21.2).

例 21.7.3 中的 $\Gamma=\{\mathscr{A},\mathscr{B}\to(\mathscr{A}\to\mathscr{B})\}$,它的演绎中的公式序列 $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_7$ 就是(1),(2),…,(7).

例 21.7.4 给出 L 中公式 $\mathscr{A}\to\mathscr{A}$ 的证明,即 $\vdash_L(\mathscr{A}\to\mathscr{A})$.

证明

(1) $(\mathscr{A}\to((\mathscr{A}\to\mathscr{A})\to\mathscr{A}))\to((\mathscr{A}\to(\mathscr{A}\to\mathscr{A}))\to(\mathscr{A}\to\mathscr{A}))$, (A2)

(2) $\mathscr{A}\to((\mathscr{A}\to\mathscr{A})\to\mathscr{A})$, (A1)

(3) $(\mathscr{A}\to(\mathscr{A}\to\mathscr{A}))\to(\mathscr{A}\to\mathscr{A})$, (1)(2)MP

(4) $\mathscr{A}\to(\mathscr{A}\to\mathscr{A})$, (A1)

(5) $\mathscr{A}\to\mathscr{A}$. (3)(4)MP

它的证明树如图 21.3.

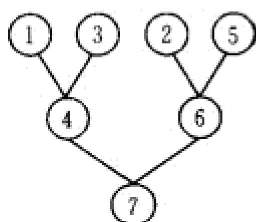


图 21.2

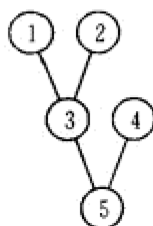


图 21.3

例 21.7.5 给出 L 中公式：$\neg\mathscr{B}\to(\mathscr{B}\to\mathscr{A})$ 的证明，即 $\vdash_L(\neg\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$.

证明

(1) $\neg\mathscr{B}\to(\neg\mathscr{A}\to\neg\mathscr{B})$, (A1)

(2) $(\neg\mathscr{A}\to\neg\mathscr{B})\to(\mathscr{B}\to\mathscr{A})$, (A3)

(3) $((\neg\mathscr{A}\to\neg\mathscr{B})\to(\mathscr{B}\to\mathscr{A}))\to(\neg\mathscr{B}\to((\neg\mathscr{A}\to\neg\mathscr{B})\to$ $\to(\mathscr{B}\to\mathscr{A})))$, (A1)

(4) $\neg\mathscr{B}\to((\neg\mathscr{A}\to\neg\mathscr{B})\to(\mathscr{B}\to\mathscr{A}))$, (2)(3)MP

(5) $(\neg\mathscr{B}\to((\neg\mathscr{A}\to\neg\mathscr{B})\to(\mathscr{B}\to\mathscr{A})))\to((\neg\mathscr{B}\to$ $(\neg\mathscr{A}\to\neg\mathscr{B}))\to(\neg\mathscr{B}\to(\mathscr{B}\to\mathscr{A})))$, (A2)

(6) $(\neg\mathscr{B}\to(\neg\mathscr{A}\to\neg\mathscr{B}))\to(\neg\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$, (4)(5)MP

(7) $\neg\mathscr{B}\to(\mathscr{B}\to\mathscr{A})$. (1)(6)MP

它的证明树如图 21.4.

21.7.1.1 关于演绎的定理

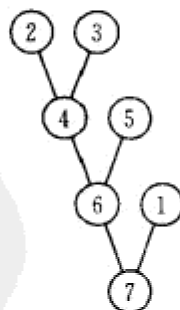


图 21.4

从上面的例子可以看出，要进行演绎或要证明一个公式是一条定理的仅有方法，是具体地写出构成证明的一个公式序列. 这常常是一件很冗长的工作. 能使定理证明变成较为容易的方法，是在证明中允许插入前面已经在 L 中证明过的公式(即定理). 另外，就是对演绎 $\vdash$ 的规则作深入的研究，引进更多的演绎规则(这些关于推

理规则的命题，有时称为**元定理**).

定理 21.7.6 (1) 若 $\Gamma\subseteq\Delta$ 且 $\Gamma\vdash\mathscr{A}$，则 $\Delta\vdash\mathscr{A}$.

(2) $\Gamma\vdash\mathscr{A}$ 的充要条件是存在 Γ 的有限子集 Δ，使得 $\Delta\vdash\mathscr{A}$.

(3) 若 $\Delta\vdash\mathscr{A}$ 且对于任意的 $\mathscr{B}\in\Delta$ 有 $\Gamma\vdash\mathscr{B}$，则 $\Gamma\vdash\mathscr{A}$.

上述定理是明显的，在进行推导时，极为有用.

下面介绍著名的演绎定理，它是 1930 年由 Herbrand 提出的.

定理 21.7.7 演绎定理(Herbrand 定理)设 Γ 是公式集，公式 $\mathscr{A},\mathscr{B}\in L$. 若 $\Gamma,\mathscr{A}\vdash\mathscr{B}$，则 $\Gamma\vdash\mathscr{A}\to\mathscr{B}$. (特别，若 $\mathscr{A}\vdash\mathscr{B}$，则 $\vdash\mathscr{A}\to\mathscr{B}$.)

证明 对构成由 $\Gamma\cup\{\mathscr{A}\}$ 到公式 $\mathscr{B}$ 的演绎序列中的公式数目(又称演绎的"深度")，用归纳法证明.

归纳基础，假设演绎序列有一个公式. 这个公式必定是 $\mathscr{B}$ 本身，因此 $\mathscr{B}$ 或者是 L 的一条公理，或者是 $\Gamma\cup\{\mathscr{A}\}$ 中的成员.

情形 1：$\mathscr{B}$ 是 L 的一条公理. 那么下面的公式序列是由 Γ 到 $\mathscr{A}\to\mathscr{B}$ 的一个演绎.

(1) $\mathscr{B}$,	L 的公理
(2) $\mathscr{B}\to(\mathscr{A}\to\mathscr{B})$,	(A1)
(3) $\mathscr{A}\to\mathscr{B}$.	(1)(2)MP

因此，$\Gamma\vdash(\mathscr{A}\to\mathscr{B})$定理得证.

情形 2：$\mathscr{B}\in\Gamma$. 下列演绎证明 $\Gamma\vdash_L(\mathscr{A}\to\mathscr{B})$.

(1) $\mathscr{B}$,	Γ 的元素
(2) $\mathscr{B}\to(\mathscr{A}\to\mathscr{B})$,	(A1)
(3) $\mathscr{A}\to\mathscr{B}$.	(1)(2)MP

情形 3：$\mathscr{B}$ 是 $\mathscr{A}$. 已经知道 $\vdash_L(\mathscr{A}\to\mathscr{A})$(见例 21.7.4)，所以公式 $\mathscr{A}\to\mathscr{A}$ 在 L 中的证明，可以作为由 Γ 到 $\mathscr{A}\to\mathscr{A}$ 的一个演绎(参见定理 21.7.6). 因此，$\Gamma\vdash(\mathscr{A}\to\mathscr{B})$. 归纳基础结束.

现在假设，由 $\Gamma\cup\{\mathscr{A}\}$ 到 $\mathscr{B}$ 的演绎是一个有 n 个公式的序列，

其中 $n>1$. 并且对所有的公式 $\mathscr{C}$,本定理都成立,这些公式 $\mathscr{C}$ 能够通过一个少于 n 个公式的序列由 $\Gamma\cup\{\mathscr{A}\}$ 演绎得到. 现分 4 种情况讨论.

情况 1:$\mathscr{B}$ 是 L 的一条公理.

情况 2:$\mathscr{B}\in\Gamma$.

情况 3:$\mathscr{B}$ 是 $\mathscr{A}$.

情况 4:$\mathscr{B}$ 由演绎中较前的两个公式,通过使用 MP 得到,这两个公式必定是 $\mathscr{C}$ 和 $\mathscr{C}\to\mathscr{B}$ 的形式,且其中每一个一定能由 $\Gamma\cup\{\mathscr{A}\}$,通过一个少于 n 个公式的序列演绎得到.

显然可见情况 1~情况 3 与归纳基础中的情形 1~情形 3 类似,现只要讨论情况 4. 这时有

$$\Gamma\cup\{\mathscr{A}\}\underset{L}{\vdash}\mathscr{C} \text{ 与 } \Gamma\cup\{\mathscr{A}\}\underset{L}{\vdash}(\mathscr{C}\to\mathscr{B}),$$

再应用归纳假设可得

$$\Gamma\underset{L}{\vdash}\mathscr{A}\to\mathscr{C} \text{ 与 } \Gamma\underset{L}{\vdash}(\mathscr{A}\to(\mathscr{C}\to\mathscr{B})).$$

最终所要求的由 Γ 到 $\mathscr{A}\to\mathscr{B}$ 的演绎如下:(演绎中公式序列标记在最左列)

$$\left.\begin{array}{l}(1)\\ \vdots\\ (k)\quad (\mathscr{A}\to\mathscr{C}),\end{array}\right\}\text{ 由 }\Gamma\text{ 到}(\mathscr{A}\to\mathscr{C})\text{的演绎.}$$

$$\left.\begin{array}{l}(k+1)\\ \vdots\\ (l)\quad \mathscr{A}\to(\mathscr{C}\to\mathscr{B}),\end{array}\right\}\text{ 由 }\Gamma\text{ 到 }\mathscr{A}\to(\mathscr{C}\to\mathscr{B})\text{的演绎.}$$

$(l+1)$ $(\mathscr{A}\to(\mathscr{C}-\mathscr{B}))\to((\mathscr{A}\to\mathscr{C})\to(\mathscr{A}\to\mathscr{B}))$, (A2)

$(l+2)$ $(\mathscr{A}\to\mathscr{C})\to(\mathscr{A}\to\mathscr{B})$, $(l),(l+1)$MP

$(l+3)$ $\mathscr{A}\to\mathscr{B}$. $(k),(l+2)$MP

所以 $\Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{B})$ 对所有情况均成立.

根据归纳法知本定理成立.

演绎定理的逆定理也是成立的.

定理 21.7.8 演绎定理的逆定理 若 $\Gamma \underset{L}{\vdash} (\mathscr{A} \to \mathscr{B})$,则 $\Gamma \cup \{\mathscr{A}\} \underset{L}{\vdash} \mathscr{B}$.

注 演绎定理又称条件证明规则(conditional proof),简记 CP. 它是可以作为系统 L 中推导命题公式的推理规则,与 MP 规则一样来使用. 与 MP 规则的不同点仅仅在于它不是初始规则而是导出规则. 它称为条件证明规则的原因,在于该定理的陈述中表明要证明结论是 $\Gamma \underset{L}{\vdash} (\mathscr{A} \to \mathscr{B})$ 时,只要证明 $\Gamma, \mathscr{A} \underset{L}{\vdash} \mathscr{B}$ 就行了. 而后者是把命题公式 $\mathscr{A}$ 当成假设(条件)添加进前提之中. 从数学文献的习惯看,是在前提中又附加了新的条件 $\mathscr{A}$. 因此称为条件证明规则. 而 $\mathscr{A}$ 也常常称为"附加条件"(或"附加假设").

此外,还有下述的推理规则.

定理 21.7.9 假言三段论规则(hypothetical syllogism, HS) 对任意公式 $\mathscr{A}, \mathscr{B}, \mathscr{C} \in L$,有

$$\{(\mathscr{A} \to \mathscr{B}), (\mathscr{B} \to \mathscr{C})\} \underset{L}{\vdash} (\mathscr{A} \to \mathscr{C}).$$

定理 21.7.10 若公式 $\mathscr{A}_1, \cdots, \mathscr{A}_n, \mathscr{A} \in L$,则

$$\mathscr{A}_1, \cdots, \mathscr{A}_n \underset{L}{\vdash} \mathscr{A} \Leftrightarrow \underset{L}{\vdash} (\mathscr{A}_1 \land \mathscr{A}_2 \land \cdots \land \mathscr{A}_n) \to \mathscr{A}.$$

在系统 L 中,增加了 GH, HS 导出规则后,可以减少推导的步骤. 看下面的例子.

例 21.7.11 给出 L 中公式: $\neg \mathscr{B} \to (\mathscr{B} \to \mathscr{A})$ 的证明,即 $\underset{L}{\vdash} (\neg \mathscr{B} \to (\mathscr{B} \to \mathscr{A}))$.

证明

(1) $\neg \mathscr{B} \to (\neg \mathscr{A} \to \neg \mathscr{B})$, (A1)

(2) $(\neg \mathscr{A} \to \neg \mathscr{B}) \to (\mathscr{B} \to \mathscr{A})$, (A3)

(3) $\neg \mathscr{B} \to (\mathscr{B} \to A)$. (1)(2)HS

例 21.7.11 与例 21.7.5 是相同的,但例 21.7.11 中由于使用了 HS 规则,使证明步骤减少了 4 步.

21.7.1.2 L 的可靠性与相容性

系统 L 是一个命题逻辑的推理系统. 我们研究了它的推导功能,也就是它的推演能力. 我们不能仅仅局限于对个别命题的推演,更重要的是从整个系统 L 角度进行研究.

(1) 在系统 L 中推导的定理(可证公式),是否为永真的命题形式(重言式).

(2) 全部永真的命题形式(重言式),是否都是系统 L 中的定理(可证公式).

上述问题涉及到形式推理系统的性能优劣和功能强弱. 研究这些问题,对形式推理系统具有重要的意义.

如果在一个形式推理系统(即逻辑演算)中推导的定理都是逻辑真命题(重言式),那么应该说这种系统,它的性能是优良的或可靠的. 如果所有的逻辑真命题(重言式),都能在这种系统中作为定理而推导出来,则应该说这个系统的推理功能是足够强的或完全的.

可靠性反映逻辑系统性质的优劣,完全性则反映逻辑系统功能的强弱.

以下将详细地研究这些问题. 首先讨论相容性.

相容性又称**无矛盾性**、**协调性**、**一致性**与**和谐性**. 它是形式系统的重要性质之一. 它有多种定义:

定义 21.7.12　古典相容性　一个公理系统是**古典相容的**(classical consistent),当且仅当不存在任何公式 $\mathscr{A}$ 使得 $\mathscr{A}$ 和 $\neg\mathscr{A}$ 都是系统中的定理.

定义 21.7.13　语法相容性　一个公理系统是**语法相容的**(syntactical consistent),当且仅当并非任一公式都在该系统中可证.

定义 21.7.14　语义相容性　一个公理系统是**语义相容的**(semantical consistent),当且仅当该系统中的一切定理(可证公

式),都是永真公式(重言式).

通过下述诸定理,可知命题演算系统 L 与谓词演算系统,在上述三种意义下都是成立的.

定理 21.7.15　可靠性定理(soundness theorem)/**有效性定理**(validity theorem)/**语义相容性定理**　L 的定理都是重言式.简略地表示为:对于任意的 $\mathscr{A}\in L$: $\underset{L}{\vdash}\mathscr{A}\Rightarrow\underset{L}{\models}\mathscr{A}$.

注　语义相容性在有些文献中又称之为可靠性或有效性(有时也称为逻辑有效性).

定理 21.7.16　相容性定理　系统 L 是相容的.

注　本定理中的相容性是兼指上述三种定义的.

21.7.1.3　L 的完全性

完全性反映形式系统推理功能的强弱,是形式推理系统的重要性质之一.它也有各种不同的定义,一般有下述三种.

定义 21.7.17　古典完全性(或简单完全性)　一个公理系统是**古典完全的**(classical completeness),当且仅当对于任一公式 $\mathscr{A}$,$\mathscr{A}$ 是定理或者 $\neg\mathscr{A}$ 是定理.

定义 21.7.18　语法完全性(或强完全性)　一个公理系统是**语法完全的**(syntactical completeness),当且仅当若把一个不是定理的公式,添加到该系统中作为公理,结果所得到的系统是不相容的(矛盾的).

定义 21.7.19　语义完全性(或弱完全性)　一个公理系统是**语义完全的**(semantical completeness),当且仅当一切属于某一特定范围内的真命题(重言式)都是该系统中的定理.

注　关于完全性详细说明如下:

(1) 古典完全性是针对不含有自由变元的公式系统,命题演算和谓词演算中的公式都含有自由变元,因此它们都没有这种完全性.

(2) 命题演算具有语法完全性,这是一种较强的完全性.但

谓词演算不具有这种完全性.

(3) 命题演算与谓词演算具有语义完全性,这是一种较弱的完全性. Gödel 在 1929 年首先证明了这种完全性,故谓词演算的完全性定理就称为 **Gödel 完全性定理**.

Gödel 完全性定理如下:

定理 21.7.20 L 的语义完全性 若公式 $\mathscr{A}\in L$ 是一个重言式(即永真公式),则 $\mathscr{A}$ 是 L 中的定理. 简记作 $\vDash \mathscr{A} \Rightarrow \underset{L}{\vdash} \mathscr{A}$.

综合定理 21.7.15 与定理 21.7.20 可知,形式系统 L 具有极为良好的性质:即在系统 L 中的定理(即可证公式)恰恰是那些"逻辑真"的公式(即永真式). L 中的公理和推理规则完全刻画了该系统的逻辑特点(既不多,也不少). 我们有下述结论:

$$\vDash \mathscr{A} \Leftrightarrow \underset{L}{\vdash} \mathscr{A}.$$

上述结论表明:在数理逻辑的研究中,已建立了纯形式的语法研究和语义研究之间的桥梁(深刻的联系). 人们既可以通过语义的研究了解语法方面的问题,也可以通过语法的研究了解语义方面的问题. 这恰如代数几何学,它在代数学与几何学之间建立的桥梁,人们可以用精巧的代数方法去研究几何,也可以用直观的几何方法去把握代数. 代数学缺少了几何直观就会迷失方向,几何学如果失去了代数学的控制,它就会泛滥成灾.

21.7.2 自然推理系统 G

自然推理系统也是一个形式推理系统,它的公理极少(或没有公理). 主要利用推理规则进行推导,这些规则也是通常思维推理的规则,如同数学中的推理. 这种推导更接近于一般的数学思维,因此称为**自然推理系统**(natural deduction system). 它是在 20 世纪 30 年代首次被 Gantzen 提出的,其后有种种变化,现在介绍的系统 G 是其中的一种.

系统 G 只有一条公理模式以及若干条推理规则. 其中联结词

与公式的定义与系统 L 完全一样.

定义 21.7.21 系统 G 定义如下:

(1) 公理模式: $\mathscr{A}\vdash\mathscr{A}$.

(2) 推理规则:

1) $\dfrac{\Gamma\vdash\mathscr{A};\ \Gamma\vdash\mathscr{B}}{\Gamma\vdash\mathscr{A}\wedge\mathscr{B}}$,

2) $\dfrac{\Gamma\vdash\mathscr{A}\wedge\mathscr{B}}{\Gamma\vdash\mathscr{A}}$, $\dfrac{\Gamma\vdash\mathscr{A}\wedge\mathscr{B}}{\Gamma\vdash\mathscr{B}}$,

3) $\dfrac{\Gamma\vdash\mathscr{A}}{\Gamma\vdash\mathscr{A}\vee\mathscr{B}}$, $\dfrac{\Gamma\vdash\mathscr{B}}{\Gamma\vdash\mathscr{A}\vee\mathscr{B}}$,

4) $\dfrac{\Gamma,\mathscr{A}\vdash\mathscr{C};\ \Gamma,\ \mathscr{B}\vdash\mathscr{C};\ \Gamma\vdash\mathscr{A}\vee\mathscr{B}}{\Gamma\vdash\mathscr{C}}$,

5) $\dfrac{\Gamma,\mathscr{A}\vdash\mathscr{B}}{\Gamma\vdash\mathscr{A}\to\mathscr{B}}$,

6) $\dfrac{\Gamma\vdash\mathscr{A};\Gamma\vdash\mathscr{A}\to\mathscr{B}}{\Gamma\vdash\mathscr{B}}$,

7) $\dfrac{\Gamma,\neg\mathscr{A}\vdash}{\Gamma\vdash\mathscr{A}}$,

8) $\dfrac{\Gamma\vdash\mathscr{A};\ \Gamma\vdash\neg\mathscr{A}}{\Gamma\vdash}$,

9) $\dfrac{\Gamma,\mathscr{A},\mathscr{B},\Delta\vdash\mathscr{C}}{\Gamma,\mathscr{B},\mathscr{A},\Delta\vdash\mathscr{C}}$,

10) $\dfrac{\Gamma\vdash\mathscr{A}}{\Gamma,\mathscr{B}\vdash\mathscr{A}}$.

注 上述定义中的大写希腊字母 $\Gamma,\Delta,\cdots$ 表示公式的有限序列(有时可能是空集).

定义 21.7.22 表达式 $\Gamma\vdash\Delta$,称为**矢列式**(sequent)其中 Γ 与 Δ 分别称为**前件(集合)**(antecedent)与**后件(集合)**(succedent).

由此定义可知,G 中的矢列式有下面 4 种:

(1) $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_n\vdash\mathscr{C}$,

(2) $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_n\vdash$,

(3) $\vdash \mathscr{C}$,

(4) $\vdash$.

分述之.

(1) 中的矢列式表示从前提：$\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n$ 可推导出结论 $\mathscr{C}$,即

$$\mathscr{A}_1 \wedge \mathscr{A}_2 \wedge \cdots \wedge \mathscr{A}_n \rightarrow \mathscr{C}.$$

是重言式.

(2) 中的矢列式表示从前提：$\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n$ 可推导出矛盾的结论,即

$$\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n \rightarrow \perp.$$

(3) 中的矢列式表示前提集是空集,从而 $\vdash \mathscr{C}$ 如系统 L 中的表示一致,即公式 $\mathscr{C}$ 是 G 中的定理(可证公式).

(4) 中的矢列式表示从空前提到空结论的推导,可知 $\vdash$ 是公理模式的一个特例.

现对系统 G 中的推理规则(定义 21.7.21)详细解释：G 中的推理规则是从矢列式到矢列式的变换规则,位于横线上的是假设,位于横线下的是结论. 规则 1)的意义是若从 Γ 可推导出 $\mathscr{A}$ 并且从 Γ 也可推导出 $\mathscr{B}$,则从 Γ 可推导出公式 $\mathscr{A} \wedge \mathscr{B}$. 规则 2)的意义是从 Γ 可推导出 $\mathscr{A} \wedge \mathscr{B}$,则从 Γ 可推导出 $\mathscr{A}$,并且从 Γ 可推导出 $\mathscr{B}$. 规则 3)是明显的. 规则 4)的意义是若公式 $\mathscr{A} \vee \mathscr{B}$ 可从 Γ 推导出来,而从 $\Gamma, \mathscr{A}$ 可推导出 $\mathscr{C}$,且从 $\Gamma, \mathscr{B}$ 可推导出 $\mathscr{C}$,则从 Γ 可推导出 $\mathscr{C}$. 规则 5)相当于系统 L 中的演绎定理. 规则 6)相当于系统 L 中的 MP 规则. 规则 7)的意义是从 $\Gamma, \neg \mathscr{A}$ 可推导出假命题,则从 Γ 可推导出 $\mathscr{A}$,它相当于系统 L 中的反证法原则. 规则 8),9)是明显的. 规则 10)的意义说明若从前提 Γ 可推导出公式 $\mathscr{A}$,则在假设中添加任何新的公式 $\mathscr{B}$,不影响推导的结论. 从上可知系统 G 减少了公理的数量而增加了推理规则,其实这些规则都是久经考验过的规律,它本身与公理并无实质上的差异. 关于系统 G 与系统 L 一样有着相容性、完全性等问题,我们不详细研究,有兴趣的读者

可看有关专著.

现在举出在 G 中推导的例子.

例 21.7.23 证明：$\vdash (P\wedge Q)\to(Q\wedge P)$.

证明

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash P\wedge Q}{\vdash Q}(2)\qquad\qquad \dfrac{\vdash P\wedge Q}{\vdash P}(2)}{\vdash Q\wedge P}(1)}{P\wedge Q\vdash Q\wedge P}(10)}{\vdash (P\wedge Q)\to(Q\wedge P)}(5)$$

注 我们把推理规则标示在横线旁，证明树如图 21.5 所示.

例 21.7.24 证明：$\vdash P\to((P\to\bot)\to\bot)$.

证明

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdash P\qquad \vdash P\to\bot}{\vdash\bot}(6)}{P\to\bot\ \vdash\bot}(10)}{\vdash(P\to\bot)\to\bot}(5)}{P\vdash(P\to\bot)\to\bot}(10)}{\vdash P\to((P\to\bot)\to\bot)}(5)$$

证明树如图 21.6 所示.

例 21.7.25 证明：$\vdash (P\to(Q\to R))\to((P\wedge Q)\to R)$.

证明

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdash P\wedge Q}{\vdash Q}(2)\qquad \dfrac{\dfrac{\vdash P\wedge Q}{\vdash P}(2)\qquad \vdash P\to(Q\to R)}{\vdash Q\to R}(6)}{\vdash R}(6)}{(P\wedge Q)\vdash R}(10)}{\vdash(P\wedge Q)\to R}(5)}{(P\to(Q\to R))\vdash(P\wedge Q)\to R}(10)}{\vdash(P\to(Q\to R))\to((P\wedge Q)\to R)}(5)$$

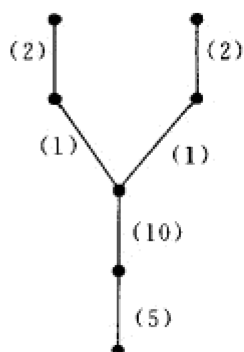


图 21.5

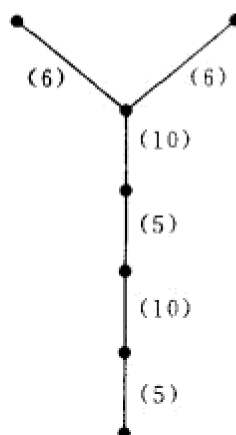


图 21.6

证明树如图 21.7 所示.

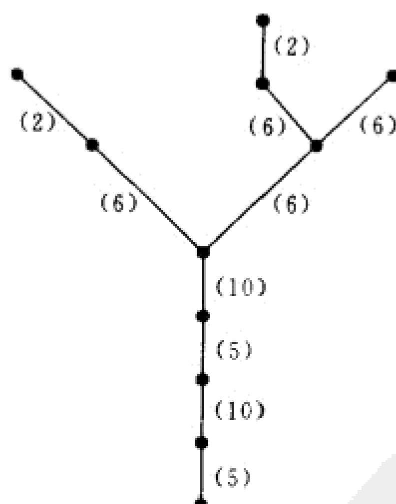


图 21.7

21.7.3 其他形式系统

由于采用不同的联结词与不同的公理,可以得到不同的命题逻辑形式公理系统.

定义 21.7.26　系统 L_1　类似于系统 L,采用如下 3 条公理:

(1) $P\to(Q\to P)$;

(2) $(P\to(Q\to R))\to((P\to Q)\to(P\to R))$;

(3) $(\neg Q\to\neg P)\to((\neg Q\to P)\to Q)$.

推理规则除 MP 规则外,还有代入规则:可允许对任意公式中的任何原子命题变元代以任何的公式.

定义 21.7.27　系统 L_2　初始联结词的功能完备集是 $\{\neg,\vee\}$,联结词"$\to$"定义如下:$\mathscr{A}\to\mathscr{B}\triangleq\neg\mathscr{A}\vee\mathscr{B}$,有 4 条公理模式:

(1) $(\mathscr{A}\vee\mathscr{A})\to\mathscr{A}$;

(2) $\mathscr{A}\to(\mathscr{A}\vee\mathscr{B})$;

(3) $(\mathscr{A}\vee\mathscr{B})\to(\mathscr{B}\vee\mathscr{A})$;

(4) $(\mathscr{B}\to\mathscr{C})\to((\mathscr{A}\vee\mathscr{B})\to(\mathscr{A}\vee\mathscr{C}))$.

推理规则为 MP 规则.

这个系统由 Hilbert-Ackermann 提出.

定义 21.7.28　系统 L_3　初始联结词的功能完备集是 $\{\neg,\wedge\}$,联结词"$\to$"定义如下:$\mathscr{A}\to\mathscr{B}\triangleq\neg(\mathscr{A}\wedge\neg\mathscr{B})$. 有 3 条公理模式:

(1) $\mathscr{A}\to(\mathscr{A}\wedge\mathscr{A})$;

(2) $(\mathscr{A}\wedge\mathscr{B})\to\mathscr{A}$;

(3) $(\mathscr{A}\to\mathscr{B})\to(\neg(\mathscr{B}\wedge\mathscr{C})\to\neg(\mathscr{C}\wedge\mathscr{A}))$.

推理规则为 MP 规则.

这个系统是由 Rosser 提出.

定义 21.7.29　系统 L_4　初始联结词的功能完备集是 $\{\neg,\to,\wedge,\vee\}$,有 10 条公理模式:

(1) $\mathscr{A}\to(\mathscr{B}\to\mathscr{A})$;

(2) $(\mathscr{A}\to(\mathscr{B}\to\mathscr{C}))\to((\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to\mathscr{C}))$;

(3) $(\mathscr{A}\wedge\mathscr{B})\to\mathscr{A}$;

(4) $(\mathscr{A}\wedge\mathscr{B})\to\mathscr{B}$;

(5) $\mathscr{A}\to(\mathscr{B}\to(\mathscr{A}\wedge\mathscr{B}))$;

(6) $\mathscr{A}\to(\mathscr{A}\vee\mathscr{B})$;

(7) $\mathscr{B}\to(\mathscr{A}\vee\mathscr{B})$;

(8) $(\mathscr{A}\to\mathscr{C})\to((\mathscr{B}\to\mathscr{C})\to((\mathscr{A}\vee\mathscr{B})\to\mathscr{C}))$;

(9) $(\mathscr{A}\to\mathscr{B})\to((\mathscr{A}\to\neg\mathscr{B})\to\neg\mathscr{A})$;

(10) $\neg\neg\mathscr{A}\to\mathscr{A}$.

这个系统是由 Kleene 提出. 它的推理规则是 MP.

定义 21.7.30　系统 Ł　系统 Ł 中的公式与系统 L 一致,该系统有 3 条公理模式:

(1) $(\neg\mathscr{A}\to\mathscr{A})\to\mathscr{A}$;

(2) $\mathscr{A}\to(\neg\mathscr{A}\to\mathscr{B})$;

(3) $(\mathscr{A}\to\mathscr{B})\to((\mathscr{B}\to\mathscr{C})\to(\mathscr{A}\to\mathscr{C}))$

它的推理规则也是 MP. 这个系统是由波兰数学家 Łukasiewicz 提出.

定义 21.7.31　系统 L_5　初始联结词是功能完备集$\{\neg,\to\}$,它仅有一条公理模式:

$$[((((\mathscr{A}\to\mathscr{B})\to(\neg\mathscr{C}\to\neg\mathscr{D}))\to\mathscr{C})\to\mathscr{C}]\to[(\mathscr{C}\to\mathscr{A})\to(\mathscr{D}\to\mathscr{A})].$$

推理规则仍为 MP.

这个系统是由 C. A. Meredith 提出.

定义 21.7.32　系统 L_6　初始联结词采用功能完备集$\{\uparrow\}$,它仅有一条公理模式:

$$(\mathscr{A}\uparrow(\mathscr{B}\uparrow\mathscr{C}))\uparrow\{[\mathscr{D}\uparrow(\mathscr{D}\uparrow\mathscr{D})]\uparrow[(\mathscr{E}\uparrow\mathscr{B})\uparrow((\mathscr{A}\uparrow\mathscr{E})\uparrow(\mathscr{A}\uparrow\mathscr{E}))]\}.$$

它也仅有一条推理规则:

$$\mathscr{A}\uparrow(\mathscr{B}\uparrow\mathscr{C}),\mathscr{A}\vdash\mathscr{C}.$$

这个系统最早由 J. Nicod 提出,非常有名.

22 标准(古典)谓词逻辑

标准(古典)谓词逻辑有许多不同的名称：谓词逻辑、一阶逻辑、初等逻辑、狭函数演算、狭谓词演算、量词理论、关系演算等等.目前较为流行的称呼是谓词逻辑与一阶逻辑.

22.1 谓词与量词

在命题逻辑推理系统中，把原子命题看作是基本单位，是不可再分的整体. 复合命题是由原子命题通过逻辑联结词来表达的. 命题逻辑的推理建立在这个层次上. 因此有些推理是无法在这个系统中表达的. 见下例.

例 22.1.1 苏格拉底论断(Socrates argument) 下列三个命题的论断

P：所有人都是要死的，

Q：苏格拉底是人，

所以 R：苏格拉底是要死的.

显然，这是一个正确的推理. 它的形式化如下：$P\wedge Q\rightarrow R$.

但是$(P\wedge Q)\rightarrow R$ 并不是命题逻辑推理系统中的永真式.

例 22.1.2 研究下面的推理.

A：所有的平方数(自然数)，都是正数，

B：9 是平方数，

所以 C：9 是正数.

这例中推理的形式化表示如下：$A\wedge B\rightarrow C$. 但它也不是命题逻辑系统中的永真式.

显然，上述两例中的论断是正确的. 但它们在命题逻辑推理系统中无法表达. 究其原因，就在于上述两例中，命题是作为不可分解的整体. 而在这两例的推理中，命题的内部逻辑结构，即主、谓结构起了主要的作用.

因此，为了提高推理能力，必须深入地分析命题的内部结构.

原子命题是自然语言中陈述语句的反映. 它的一般结构可概括为：

主语＋谓语

表示主语的客体，称为**主词**或**个体词**(individual)，表示谓语的词，一般是描述客体的**性质**(property)或多个客体之间的**关系**(relation). 统称为**谓词**(predieate). 下面为严格的定义.

定义 22.1.3 设任意集$\cup$与集$B=\{\top,\bot\}$，函数$P:\cup^n\to B$，称为$\cup$上的 n **元谓词**(predicate)，记作：$P(x_1,\cdots,x_n)$. 其中$x_1,\cdots,x_n$称为**个体变元**(individual variable)，$P\underbrace{(\cdot,\cdots,\cdot)}_{n}$称为谓词. 表示个体$x$性质的谓词，记作$P(x)$.

一般也用大写拉丁字母如$F,G,\cdots$表示谓词，如$F(x_1,\cdots,x_n)$. 但括号内个体词的位置不能任意改动，否则就会改变谓词的意义. 例如

$F(x,y,z)\triangleq$“$x+y>z$”,

$F(y,z,x)\triangleq$“$y+z>x$”,

显然　$F(x,y,z)\neq F(y,z,x)$.

关于谓词，还有如下的定义.

定义 22.1.4 设任意集$\cup$,$R\subseteq\cup^n$，称R为n元关系或n元**谓词**.

对于任意集$\cup$与n,n元谓词与n元关系之间是1-1对应的. 事实上：

(1) 对于n元关系R，有n元谓词P与之对应，使得

$$P(a_1,\cdots,a_n)=\mathrm{T} \quad \Leftrightarrow \quad \langle a_1,\cdots,a_n\rangle\in R.$$

(2) 对于 n 元谓词 $P(x_1,\cdots,x_n)$，有 n 元关系 R 与之对应，使得

$$\langle a_1,\cdots,a_n\rangle\in R \quad \Leftrightarrow \quad P(a_1,\cdots,a_n)=\mathrm{T}.$$

由此可知，关于谓词的两个定义是等价的. 粗略地说：谓词就是关系，关系就是谓词(性质就是一元关系).

例 22.1.5 考察下面的论断. 哪些是命题？哪些不是命题？

(1) $5=3$；

(2) $x=3$；

(3) $x\leqslant y$；

(4) $7<12$；

(5) $x+y=z$；

(6) $f(x)=0$；

(7) n 是偶数；

(8) $\varepsilon>0$；

(9) $\frac{1}{n}<\varepsilon$；

(10) x 是白的.

现在对个体词的变域不加限制. 对上例进行研究. 显然(1)中的 $5=3$ 表示命题，它是一个假命题. (2) 中的 $x=3$ 则不表示命题，因为它包含有变元 x，当 x 表示自然数 3 时，(2) 中的 $x=3$ 就变成了 $3=3$，则是一个真命题. 倘若 x 表示圆周率 π 时，(2) 中的 $x=3$ 就变成了 $\pi=3$，这时它就是一个假命题. 所以它不是命题. (3) 中的 $x\leqslant y$ 与(5)，(6)，(10) 中的论断均包含有变元 x，y，它们都不是命题. 对于(7)，(8)，(9) 诸论断，乍看起来，不出现诸如 x,y 的变元. 但它们都含有 n,ε 等参数，这些参数有时是任意的，有时又是固定的. 所以(7)，(8)，(9)严格地说，也不表示命题. 命题在任何时候都仅能通过非真即假的陈述句来表达.

因此上例中的(2),(3),(5),(6),(7),(8),(9),(10)均表示谓词.

从上例可知,一般而言包含变元的论断就如同数学中包含变元或参数的函数一样,它们都是谓词,当变元或参数的取确定值后,它们就变成了命题,因此有些文献中就说谓词是**命题函数**(propositional function).

注 由于近年来谓词逻辑在离散数学与计算机科学中大量应用,在各种书籍及文献中有许多不同的称谓,列表如下,供参考.

表 22.1

谓　词	命　题
谓词形式	真值函数
关系	不含变元的谓词
命题函数	不带参数的谓词
带变元的命题	零元谓词
带参数的命题	命题形式
开命题	闭命题

有了谓词概念后,就可以把例 22.1.5 中的某些论断通过谓词表示出来.

例 22.1.6 把例 22.1.5 中的论断形式化如下:

设谓词如下:

equ(·):“ · 等于 3”;

$\leqslant$(· , *):“ · 不大于 * ”;

$=$(· ,0):“ · 等于零”;

F(· , * ,∘):“ · + * =∘”;

E(·):“ · 是偶数”;

$<$(· , *):“ · 小于 * ”;

WHITE(·):“ · 是白色的.”

于是

(1) equ(5)（即“$5=3$”） 是命题；

(2) equ(x)（即“$x=3$”） 是谓词；

(3) $\leqslant(x,y)$（即“$x\leqslant y$”） 是二元谓词；

(4) $<(7,12)$（即“$7<12$”） 是命题；

(5) $F(x,y,z)$（即“$x+y=z$”）是三元谓词；

(6) $=(f(x),0)$（即“$f(x)=0$”）是谓词；

(7) $E(n)$（即“n 是偶数”）是谓词（当 n 变动时），是命题（当 n 确指时）；

(8) $<(0,\varepsilon)$（即“$\varepsilon>0$”）是谓词（当 ε 变动时），是命题（当 ε 固定时）；

(9) $<\left(\frac{1}{n},\varepsilon\right)$ $\left(\text{即“}\frac{1}{n}<\varepsilon\text{”}\right)$解释同(8)；

(10) WHITE(x)（即“x 是白色的”）是谓词.

在谓词逻辑中，除了个体词、谓词以外，另一个重要概念就是量词，它是如此的重要，以致于有些文献中把谓词逻辑就称作**量词理论**(quantification theory).

定义 22.1.7 谓词逻辑中表示数量的词称为**量词**(quantifier). 量词可分为**全称量词**(universal quantifier)及**存在量词**(existential quantifier). 如下：

(1) $(\forall x)$：所有的 x；
：任意的 x；
：每一个 x.

(2) $(\exists x)$：有些 x；
：存在 x；
：至少有一个 x.

(3) $(\exists!\, x)$：存在唯一的 x；
恰有一个 x.

注 对于量词亦有种种不同的表示，如表 22.2.

表 22.2

全称量词	$\forall$	$\forall x$	Ax	(x)	Πx	$\underset{x}{\wedge}$
存在量词	$\exists$	$\exists x$	$\mathrm{E}x$		Σx	$\underset{x}{\vee}$

对个体词、谓词、量词形式化之后，就可以将自然语言中表达的论断在谓词逻辑系统中表示出来.

例 22.1.8 把下述命题形式化.

(1) 所有的人都是要死的.

(2) 每一个苹果都是红的.

(3) 任意整数不是正数就是负数.

(4) 有些人是聪明的.

(5) 有些实数是有理数.

设立谓词如下：

$M(\cdot)$：· 是人.

$A(\cdot)$：· 是苹果.

$Z(\cdot)$：· 是整数.

MORTAL(·)：· 是要死的.

CLEVER(·)：· 是聪明的.

POS(·)：· 是正数.

NEG(·)：· 是负数.

$R(\cdot)$：· 是实数.

$Q(\cdot)$：· 是有理数.

RED(·)：· 是红色的.

上述命题形式化后如下：

(1′) $(\forall x)M(x)$.

(2′) $(\forall x)R(x)$.

(3′) $(\forall x)(\mathrm{POS}(x) \vee \mathrm{NEG}(x))$.

(4′) $(\exists x)\mathrm{CLEVER}(x)$.

(5′) $(\exists x)Q(x)$.

应当注意的是，在命题(1′)—(5′)中，个体变元分属于各个不同的论域(变化范围). 详言之应写成

(1″) $(\underset{x\in\{人\}}{\forall} x)M(x)$.

(2″) $(\underset{x\in\{苹果\}}{\forall} x)\mathrm{RED}(x)$.

(3″) $(\underset{x\in\mathbf{Z}}{\forall} x)(\mathrm{POS}(x) \vee \mathrm{NEG}(x))$.

(4″) $(\underset{x\in\{人\}}{\exists} x)\mathrm{CLEVER}(x)$.

(5″) $(\underset{x\in\mathbf{R}}{\exists} x)Q(x)$.

但是，要同时研究命题(3″)与(5″)时，比如下面的命题：

$$(\underset{x\in\mathbf{R}}{\exists} x)Q(x) \wedge (\underset{x\in\mathbf{Z}}{\forall} x)(\mathrm{POS}(x) \vee \mathrm{NEG}(x)) \wedge (\underset{x\in\{人\}}{\exists} x)\mathrm{CLEVER}(x),$$

由于对命题的不同部分变元 x 要取自不同的论域，产生不便. 这时可把谓词的论域扩大到集合 $S=\mathbf{R}\cup\mathbf{Z}\cup\{人\}$上，由此上面谓词的形式要起变化，表示成：

$$(\underset{x\in S}{\exists} x)[R(x) \wedge Q(x)] \wedge (\underset{x\in S}{\forall} x)(Z(x) \rightarrow (\mathrm{POS}(x) \vee \mathrm{NEG}(x)) \wedge (\underset{x\in S}{\exists} x)(M(x) \wedge \mathrm{CLEVER}(x)),$$

其中 $Z(x)$："x 是整数"，

$R(x)$："x 是实数"，

$M(x)$："x 是人".

换言之，在论域扩大的情况下，就会增加新的谓词；反之，就会减少谓词.

其实在例 22.1.8 的(1″)—(5″)中，位于量词下面的 $x\in\{人\}$，$x\in\{苹果\}$，$x\in\mathbf{Z}$，$x\in\mathbf{R}$ 也都是谓词. 即

$\mathrm{MEN}(x)$：$x\in\{人\}$，

$A(x)$：$x\in\{苹果\}$，

$Z(x)$：$x \in \mathbf{Z}$，

$R(x)$：$x \in \mathbf{R}$.

所以在最广论域$\bigcup$与受限论域 $S(S \subseteq \bigcup)$间有下面的关系：

$$(\forall_{x \in S} x)F(x) = (\forall_{x \in \bigcup} x)(S(x) \rightarrow F(x)) = (\forall x)(S(x) \rightarrow F(x)),$$

$$(\exists_{x \in S} x)F(x) = (\exists_{x \in \bigcup} x)(S(x) \wedge F(x)) = (\exists x)(S(x) \wedge F(x)),$$

其中 $S(x)$："$x \in S$"是谓词，对于最广论域，通常可省去 $x \in \bigcup$的表示.

在进行理论研究时，常采用最广论域$\bigcup$，在应用领域内则常常限制个体变元的论域，这样可使谓词公式更加简单.

例 22.1.9　苏格拉底论断（续）

设立下面的谓词：

MAN(·)："·是人"，

MORTAL(·)："·是要死的"，

s：socrates.

于是上述论断表示如下：

$((\forall x)(\mathrm{MAN}(x) \rightarrow \mathrm{MORTAL}(x)) \wedge \mathrm{MAN}(s)) \rightarrow \mathrm{MORTAL}(s)$.

可以证明上面的谓词公式是永真式. 类似地可知，例 22.1.2 也可同样地形式化而与本例完全一致.

个体词、谓词、量词形式化之后，对于任意的论断都可以形式化，并且在谓词逻辑的形式系统内进行推理.

例 22.1.10　把下列命题形式化.

(1) 所有的素数都是自然数.

(2) 对于一切实数 x,y 均有：$x+y=y+x$.

(3) 数列$\{a_n\}$是单调增数列.

(4) 对于一切实数 x 都有：$x+1>x$.

解 对于(1)，设定谓词：

$P(\cdot)$："$\cdot$是素数"，

$N(\cdot)$："$\cdot$是自然数"，

于是有 $(\forall x)(P(x)\rightarrow N(x))$.

对于(2)，(3)，(4)它们都含有数学中常用的谓词"$=$"，"$>$"，"$\geqslant$"，因此可以直接写出

(2′) $(\forall_{x\in\mathbf{R}} x)(\forall_{y\in\mathbf{R}} y)(x+y=y+x)$.

(4′) $(\forall_{x\in\mathbf{R}} x)(x+1>x)$.

(3′) $(\forall_{n\in\mathbf{N}} n)(a_{n+1}\geqslant a_n)$.

例 22.1.11 设论域是实数集 $\mathbf{R}$ 时，把下列命题符号化.

(1) 对于任意的实数 x 与 y，有实数 z 满足：$x+y=z$.

(2) 没有比零小的自然数.

(3) 对于一切实数 x，有 $x+0=x$.

(4) 对任何实数 x 与 y 均有 $x\cdot y=y$.

(5) 有实数 x，使得 $x\cdot y=y$ 对一切实数成立.

解 引入谓词：

$S(x,y,z)$："$x+y=z$"，

$M(x,y,z)$："$x\cdot y=z$"，

$N(x)$："x 是自然数"，

$L(x)$："x 小于零".

上面的命题可形式化如下：

(1′) $(\forall x)(\forall y)(\exists z)S(x,y,z)$.

(2′) $\neg(\exists x)(N(x)\wedge L(x))$.

(3′) $(\forall x)S(x,0,x)$.

(4′) $(\forall x)(\forall y)M(x,y,y)$.

(5′) $(\exists x)(\forall y)M(x,y,y)$.

注 (1) 在一个命题中含有多个量词时，量词对谓词的作用是从里往外扩展的，例如

$$(\exists x)(\forall y)M(x,y,y)=(\exists x)((\forall y)M(x,y,y)),$$

但按照惯例常省去量词之间的括号.

(2) 量词之间的先后次序是不能任意交换的，例如，下面两个命题

$$(\underset{x\in\mathbf{R}}{\forall} x)(\underset{y\in\mathbf{R}}{\exists} y)(x+y=0),$$

$$(\underset{y\in\mathbf{R}}{\exists} y)(\underset{x\in\mathbf{R}}{\forall} x)(x+y=0)$$

是两个完全不同的命题，前者是一个真命题，而后者是一个假命题.

例 22.1.12 设论域是实数集 $\mathbf{R}$，则下列公式的解释如下：

(1) $(\exists x)P(x)$：存在 x 有性质 P.

(2) $(\forall y)P(y)$：所有的 y 有性质 P.

(3) $(\forall x)(\exists y)(x=2y)$：对于所有的 x，有 y 是 x 的一半.

(4) $(\forall \epsilon)\left(\epsilon>0\rightarrow(\underset{n\in\mathbf{N}}{\exists} n)\left(\frac{1}{n}<\epsilon\right)\right)$：对所有的正实数 ϵ，存在有自然数 n，使得 $\frac{1}{n}<\epsilon$.

(5) $(x<y)\rightarrow(\exists z)((x<z)\wedge(z<y))$：若 $x<y$，则存在 z 使得 $x<z$ 且 $z<y$.

22.2 函数，项与合式公式(谓词公式)

现在可以利用逻辑联结词、谓词与量词构成谓词公式(命题函数).

定义 22.2.1 满足下列条件的表达式称为项(term)：

(1) 任意个体常量(元)或个体变量(元)是项.

(2) 若 f 是一个 n 元函数，$t_1,\cdots,t_n$ 是项，则 $f(t_1,\cdots,t_n)$ 也

是项.

(3) 仅由有限项使用(1),(2) 产生的表达式才是项.

例 22.2.2 设 f 是二元函数,g 是三元函数,a 是常量,x 是变量(元),则

(1) a 是项.(因为 a 是常量.)

(2) x 是项.(因为 x 是变量.)

(3) $f(a,x)$是项.(因为 a 与 x 都是项,并且 f 是二元函数.)

(4) $g(x,f(a,x),a)$是项.(因为 $x,f(a,x),a$ 都是项,并且 g 是三元函数).

(5) $g(a,f(a,a),a)$也是项.

不含变元的项,有时称为**闭项**(closed term).

由例 22.2.2 可知,不要混淆函数与项的概念,函数是个体域到个体域的映射;而项则是映射的值,它是个体域中的元素,简略地说就是个体域上的函数表达式,有些文献中称它是个体域中元素的"名称",它相当于自然语言中的名词或代词.

定义 22.2.3 若 P 是一个 n 元谓词,$t_1,\cdots,t_n$ 是项,则称 $P(t_1,\cdots,t_n)$为**原子公式**(atomic formula).

定义 22.2.4 满足下列条件的表达式,称为**合式公式**(well-formed formula/wff).

(1) 原子公式是合式公式.

(2) 若 $\mathscr{A}$ 是合式公式,则$(\neg\mathscr{A})$是合式公式.

(3) 若 $\mathscr{A}$ 与 $\mathscr{B}$ 是合式公式,则$(\mathscr{A}\wedge\mathscr{B})$,$(\mathscr{A}\vee\mathscr{B})$,$(\mathscr{A}\rightarrow\mathscr{B})$,$(\mathscr{A}\leftrightarrow\mathscr{B})$也是合式公式.

(4) 若 $\mathscr{A}$ 是合式公式,则$(\forall x)\mathscr{A}$,$(\exists x)\mathscr{A}$ 也是合式公式.

(5) 仅由(1)—(4) 产生的表达式才是合式公式.

其中 $\mathscr{A}=\mathscr{A}(x_1,\cdots,x_n)$,$\mathscr{B}=\mathscr{B}(x_1,\cdots,x_n)$,$n\geqslant 0$,当 $n=0$ 时的合式公式就是命题.

以后所指的命题函数、开命题、谓词、谓词公式、合式公式、公

式都是同义词，在不引起混淆时，简称谓词公式或公式.

由定义可知，合式公式是一个开命题，它的表达式里既有变量又有谓词与量词，量词的作用是对变元加以约束和限制，受到量化的变元就失去了变元的作用，通常把这种变元叫做**哑变元**(dummy variable).

下面给出有关合式公式的几个重要概念.

定义 22.2.5 设合式公式含有下列形式的子公式

$$(\forall x)\mathscr{A} \quad 或 \quad (\exists x)\mathscr{A},$$

这些子公式称为该合式公式中变元 x **受约束的部分**(x-bound part of the formula)，子公式 $\mathscr{A}$ 称为量词的**辖域**(scope).

定义 22.2.6 合式公式中的变元 x 若出现在 x 受约束的部分，则称变元 x **约束出现**(bound occurrence). 若不是约束出现，则称它是**自由出现**(free occurrence). 变元 x 在公式中约束出现时，称为**约束变元**(bound variable)，变元 x 在公式中自由出现时，称为**自由变元**(free variable).

紧接着量词的子公式，一般要用括号括起来，只有在子公式是原子公式时括号才能省去，例如：

(1) $(\forall x)\underline{P(x,y)}$；

(2) $(\forall x)\underline{(P(x,y)\to Q(x))}$；

(3) $(\forall x)\underline{(P(x)\to(\exists y)R(x,y))}$；

(4) $(\forall x)\underline{(P(x)\to R(x))}\vee(\forall x)\underline{(P(x,y)\to Q(x,y))}$；

(5) $(\exists x)\underline{(P(x)\wedge Q(x))}$；

(6) $(\exists x)\underline{P(x)}\wedge Q(x)$；

(7) $(\exists y)\underline{((\forall x)(P(x,y)\to(\forall x)Q(x)))}$.

以上公式中各量词的辖域均下加横线标出. 由定义 22.2.6 可知，在公式中，某个变元可以既是约束的，又是自由的. 例如：

$$(\forall x)P(x,y)\wedge(\forall y)Q(y),$$

其中变元 y 既是约束的，又是自由的. 这在研究问题时，会引起歧

义. 因此有换名规则.

规则 22.2.7　约束变元换名规则

(1) 可以把量词中的作用变元及相应于该量词辖域中的全部约束变元,用新的个体变元替换.

(2) 新变元是原公式中未曾出现过的.

规则 22.2.8　自由变元换名规则

(1) 可以把公式中所有的自由变元用新的个体变元替换.

(2) 新变元是原公式中未曾出现过的.

例 22.2.9　根据变元换名规则下列公式:

(1) $(\forall x)P(x,y)\wedge(\forall y)Q(y)$;

(2) $(\forall x)P(x,y)\wedge(\forall z)Q(z)$;　　(约束变元换名)

(3) $(\forall x)P(x,z)\wedge(\forall y)Q(y)$;　　(自由变元换名)

(4) $\int_a^x f(x)\mathrm{d}x=\int_a^x f(t)\mathrm{d}t$;　　(约束变元换名)

(5) $\sum_{i=1}^{n}u_i=\sum_{k=1}^{n}u_k$.　　(约束变元换名)

其中公式(1) ~(3) 是等值的,公式(4) ,(5) 是成立的.

22.3　结构,可满足性,真值,模型

命题演算中的公式,当其中的原子命题的"真"、"假"值确定之后,该公式的真、假值也随之确定. 然而在谓词逻辑中,由于有了个体词、谓词及量词后,情况要复杂得多,谓词公式,也就是开命题,其中是含有变元(个体变元)的,谓词本身也是抽象的,可以有不同的解释,此外还有不同的量词,因此,如何判断一个公式的真假,要比命题逻辑复杂得多.

例 22.3.1　判断公式:$(\exists x)(\forall y)(P(x,y)\rightarrow Q(x,y))$的真假.

解 设论域(个体域)为 $\mathbf{N}^+$,谓词设定为:

(1) $P(x,y)$:"$y>x$",

$Q(x,y)$:"$y\geqslant 1$",

则原公式是一个真命题.

若谓词设定为:

(2) $P(x,y)$:"$y\neq x$",

$Q(x,y)$:"$y=x$",

则原公式是一个假命题.

换言之,在论域 $\mathbf{N}^+$ 中,公式的真假,依赖于对谓词的不同解释(即不同的含义).

但是即使给谓词以确定的含义后,例如设定谓词 $P(x,y)$,$Q(x,y)$如前述的(1). 若选定论域为 $\mathbf{R}$(实数集),而不是 $\mathbf{N}^+$,这时原公式就变成一个假命题了.

例 22.3.2 判断公式 $P(x,y)\to Q(x,y)$的真假.

解 由于公式是一个开命题,这时设论域为 $\mathbf{N}$,设 $P(x,y)$"$x+y=0$",$Q(x,y)$:"$x>y$".

这时,如果给变量赋值,令 $x=1,y=2$,则原命题为真;如果令 $x=y=0$,则原命题为假.

从上面的例题可知,对于谓词公式,当它是闭命题时,在论域确定时,该命题的真假值依赖于谓词的含义而不同;当它是开命题时,则不但随论域的不同,谓词的含义不同,而且还与变量的赋值不同有关.

一般而言,对于任意的谓词公式,它们的真假值依赖于:

(1) 论域;

(2) 个体常元的值;

(3) 个体变元的赋值(函数);

(4) 函数符号的含义;

(5) 谓词符号的含义.

只有在上述5个条件都满足时，才能确定它们的真假值.

因此，对于任何一个谓词公式，或是谓词演算系统中的谓词公式集，要想确定其中公式的真假，就要有一个确定的(或有组织的)集合，以它作为论域，在其上有确定的函数、关系，以及确定的常元. 这样的集合称为数学结构，定义如下.

定义 22.3.3 一个**数学结构**(mathematical structure) 是一个四元组 $\mathscr{D}$:

$$\mathscr{D}=\langle D,\{\overline{R}_i\}_{i\in I},\{\overline{f}_j\}_{j\in J},\{\overline{c}_k\}_{k\in K}\rangle.$$

以及映射：λ: $I\to\mathbf{N}^+$，μ: $J\to\mathbf{N}^+$ 使得：

(1) $\mathscr{D}$ 的论域是 D，为一非空集合；

(2) 定义在 D 上的关系集合 $\{\overline{R}_i\}_{i\in I}$，$\overline{R}_i$ 是 $\lambda(i)$元关系；

(3) 定义在 D 上的函数集合 $\{\overline{f}_j\}_{j\in J}$，$\overline{f}_j$ 是 $\mu(j)$元函数；

(4) D 中的特殊元素(常元)集 $\{\overline{c}_k\}_{k\in K}$.

例 22.3.4 判断下列公式的真假：

(1) $R(x_1,x_2)$.

(2) $(\forall x_2)R(x_1,x_2)$.

(3) $(\exists x_2)(\forall x_1)R(x_2,x_1)$.

解 设论域为 $\mathbf{N}^+$，谓词 $R(y,z)$：“$y\leqslant z$”. 这时

(1) 就是谓词 $R(x_1,x_2)$，是 $x_1\leqslant x_2$，如果给变量 $x_1=1$，$x_2=2$，则 $R(1,2)$是真命题. 如果给变量 $x_1=2$，$x_2=1$，则 $R(2,1)$就是假命题.

(2) 则表示性质：“对于所有的正整数 z 有性质 $y\leqslant z$”，这仅当 $y=1$ 时是真命题.

(3) 是一个闭公式，它表示性质：“存在一个最小的正整数”，所以它是一个永真命题.

例 22.3.5 判断下列公式的真假.

(1) $P(x)\to P(a)$ (a 是常元).

(2) $(\exists x)A(x)\to(\forall x)A(x)$.

解 给定结构如下：

$$\mathcal{N}=\langle \mathbf{N},\{\overline{P}(x),\overline{A}(x)\},\overline{0}\rangle,$$

其中，N 是自然数集，$\overline{P}(x)$，$\overline{A}(x)$是如下的关系：

$$\overline{P}(x):\text{“}x>0\text{”},$$

$$\overline{A}(x):\text{“}x\leqslant 0\text{”},$$

$$\overline{0}:\text{“自然数零”}.$$

把公式(1)，(2) 中的常元解释成 $\mathcal{N}$ 中的 $\overline{0}$，谓词 $P(x)$，$A(x)$ 分别解释成 $\overline{P}(x)$，$\overline{A}(x)$，于是公式(1) (2) 分别解释成：

(1′) $\overline{P}(x)\to\overline{P}(\overline{0})$，即$(x>0)\to(0>0)$.

(2′) $(\exists x)\overline{A}(x)\to(\forall x)\overline{A}(x)$，即$(\exists x)(x\leqslant 0)\to(\forall x)(x\leqslant 0)$.

公式(2′)是一个闭命题，而且是一个假命题. 公式(1′)是一个开命题，它的真假还视对变量的赋值而定.

由上述例子可知，对于任意的谓词公式，只有在给定结构以及对变量的赋值之后，才能确定它的真假值. 是否有对一切结构以及一切赋值均取真值的谓词公式呢？看下面的例子.

例 22.3.6 判断下列公式的真假：

(1) $(\forall x)(\forall y)(P(x,y)\wedge Q(x,y)\to P(x,y))$.

(2) $\neg P(x,y)\vee P(x,y)$.

解 公式(1)，(2) 无论在何种结构中，无论对变元作何种赋值，它们均取真值. 这是由于对任意的命题变元 p,q 而言，公式

$$p\wedge q\to p,$$

$$\neg p\vee p$$

恒取真值，而把谓词 $P(x,y)$，$Q(x,y)$分别代入 p,q 就得到公式(1)，(2)，同时它们关于一切结构与一切赋值恒取真值.

现在我们给出可满足性、真与模型的严格定义及其性质.

定义 22.3.7 结构 $\mathcal{D}$ 上的一个**赋值**(valuation)是一个从项集到 $\mathcal{D}$ 中基集 D 的具有下述性质的函数 v：

(1) $v(c_k)=\overline{c}_k$，对于每个常元 c_k，

(2) $v(f_j(t_1,\cdots,t_n))=\overline{f}_j(v(t_1),\cdots,v(t_n))$，

其中 f_j 是任意的函数符号，$t_1,\cdots,t_n$ 是项.

由上定义可知赋值是一个规则，它对于每一个项，指派了 D 中的一个元素作为它的解释.

注 (1) 一般情形，在一给定的结构中，会有多种不同的赋值.

(2) 一个给定的赋值，对于每个变元 x_i，指派 D 中的一个元素与之对应. 换言之，赋值 v 可以通过一个无穷序列：$v(x_1)$，$v(x_2)$，…而完全确定. 而由 D 中可列个元素构成的序列组成的集合常记作 Σ，因此 $v\in\Sigma$.

定义 22.3.8 设 $v,v'\in\Sigma$，若

$$v(x_j)=v'(x_j)\text{，当 } j\neq i$$

则称 v,v' 是**几乎相等的赋值**(almost equivalent).

注意，几乎处处相等的赋值，除在 x_i 处可能不等外，对其他的变元都有相同的值.

定义 22.3.9 设 $\mathscr{A}$ 是一公式，$\mathscr{D}$ 是一个结构，任意赋值 $v\in\Sigma$，若满足下述条件，则称**在 $\mathscr{D}$ 中赋值 v 满足公式 $\mathscr{A}$**(v satisfies $\mathscr{A}$ in $\mathscr{D}$). 记作 $\mathscr{D}\models_v\mathscr{A}$.

(1) 当 $\mathscr{A}$ 是原子公式时，即 $\mathscr{A}=P(t_1,\cdots,t_n)$，则

$\mathscr{D}\models_v P(t_1,\cdots,t_n) \quad\Leftrightarrow\quad \langle v(t_1),\cdots,v(t_n)\rangle\in\overline{P}$；

(2) $\mathscr{D}\models_v\neg\mathscr{A} \quad\Leftrightarrow\quad \mathscr{D}\not\models_v\mathscr{A}$；

(3) $\mathscr{D}\models_v(\mathscr{B}\to\mathscr{C}) \quad\Leftrightarrow\quad \mathscr{D}\models_v\neg\mathscr{B}$ 或者 $\mathscr{D}\models_v\mathscr{C}$；

(4) $\mathscr{D}\models_v(\forall x_i)\mathscr{B} \quad\Leftrightarrow\quad \forall v'\in\Sigma,\mathscr{D}\models_{v'}\mathscr{B}$.

注 (1) 对任何公式 $\mathscr{A}$，任何赋值 v，或者 $\mathscr{D}\models_v\mathscr{A}$ 或者 $\mathscr{D}\models_v\neg\mathscr{A}$.

(2) 公式$(\forall x_i)\mathscr{B}$ 可解释为某个命题"对于任意的 $y\in D$…"，在此 x_i 解释成 y(D 中的任意元素)，赋值 v 对于出现在 $\mathscr{B}$ 中的变元进行了赋值，因此如果 v 满足 $\mathscr{B}$，而且 v 通过改变 $v(x_i)$ 而得的

任意几乎处处相等的赋值也满足 $\mathscr{B}$,则 v 满足 $(\forall x_i)\mathscr{B}$ 当然是正确的.

定理 22.3.10 对于任意的公式 $\mathscr{A},\mathscr{B}$,任意的结构 $\mathscr{D}$ 以及任意的赋值 $v\in\Sigma$,有:

(1) $\mathscr{D}\models_v\mathscr{A}\wedge\mathscr{B} \iff \mathscr{D}\models_v\mathscr{A}$ 并且 $\mathscr{D}\models_v\mathscr{B}$;

(2) $\mathscr{D}\models_v\mathscr{A}\vee\mathscr{B} \Leftrightarrow \mathscr{D}\models_v\mathscr{A}$ 或者 $\mathscr{D}\models_v\mathscr{B}$;

(3) $\mathscr{D}\models_v\mathscr{A}\leftrightarrow\mathscr{B} \Leftrightarrow \mathscr{D}\models_v\mathscr{A}$ 同时 $\mathscr{D}\models_v\mathscr{B}$;

(4) $\mathscr{D}\models_v(\exists x_i)\mathscr{A} \Leftrightarrow \exists v'\in\Sigma,\mathscr{D}\models_{v'}\mathscr{A}$.

这里 v' 与 v 几乎处处等值.

定义 22.3.11 若在结构 $\mathscr{D}$ 中任意的赋值都满足 $\mathscr{A}$,则称公式 $\mathscr{A}$ 在结构 $\mathscr{D}$ 中是**真**的(true),记作 $\mathscr{D}\models\mathscr{A}$. 若不存在 $\mathscr{D}$ 中满足 $\mathscr{A}$ 的任意赋值,则称 $\mathscr{A}$ 在 $\mathscr{D}$ 中是**假**的(false).

公式 $\mathscr{A}$ 在某个结构 $\mathscr{D}$ 中是真的(即 $\mathscr{D}\models\mathscr{A}$),有时也称为**解释真**(true in an interpretation).

定理 22.3.12 若 $\mathscr{D}\models\mathscr{A}$ 并且 $\mathscr{D}\models\mathscr{A}\to\mathscr{B}$,则 $\mathscr{D}\models\mathscr{B}$.

定理 22.3.13 设 $\mathscr{A}$ 是任意的公式,$\mathscr{D}$ 是任意的结构,则 $\mathscr{D}\models\mathscr{A}$ 的充要条件是 $\mathscr{D}\models(\forall x_i)\mathscr{A}$,其中 x_i 是任意变元.

注 这个定理在数学中经常使用,有时甚至于达到不自觉的程度. 首先,对 $\mathscr{A}$ 中并不自由出现的变元加以量化后得 $(\forall x_i)\mathscr{A}$,实质上并没有改变 $\mathscr{A}$ 的解释,因此这时 $\mathscr{A}$ 真的充要条件就是 $(\forall x_i)\mathscr{A}$ 真. 其次,对 $\mathscr{A}$ 中自由出现的变元加量词得出 $(\forall x_i)\mathscr{A}$,就说明公式中的 x_i 已成为哑变元. 上述定理表明:考查含有自由变元的公式的真假值时,就意味着在公式前的全称量词被省略了.

定理 22.3.14 设 $\mathscr{A}$ 是任意的闭公式,$\mathscr{D}$ 是任意的解释,则 $\mathscr{D}\models\mathscr{A}$ 或 $\mathscr{D}\models\neg\mathscr{A}$.

该定理说明,对于闭公式,它的真假与 $\mathscr{D}$ 中的赋值已无关系.

另有下面的重要定义.

定义 22.3.15 (1) 若公式 $\mathscr{A}$ 在任意结构 $\mathscr{D}$ 中是真的,则称

$\mathscr{A}$是**逻辑有效的**(或普效的/有效的)(logically valid).

(2) 若$\neg\mathscr{A}$是普效的,则称$\mathscr{A}$为**矛盾的**(contradictory).

(3) 若至少有一个结构以及至少有一种赋值满足$\mathscr{A}$,则称$\mathscr{A}$是**可满足的**(satisfiable).

定义 22.3.16 设Γ是公式集,$\mathscr{D}$是一结构,若Γ中的任意公式在$\mathscr{D}$中都是真的,则称$\mathscr{D}$是Γ的**模型**(model),记作$\mathscr{D}=(\mathrm{Mod})\Gamma$.

22.4 谓词公式(命题函数)与等值演算

与命题逻辑类似,现在给出谓词逻辑中等值演算的重要定理.首先已知在命题逻辑中的一大批永真式可以适当地移植到谓词逻辑中来.

定义 22.4.1 设命题逻辑中的合式公式为$\mathscr{A}$,$x_i(1\leqslant i\leqslant n)$是$\mathscr{A}$中的命题变元,现用任意的谓词公式$\mathscr{A}_i(1\leqslant i\leqslant n)$,分别代入$x_i$后得到的合式公式:

$$\mathscr{A}_{x_1,\cdots,x_n}^{\mathscr{A}_1,\cdots,\mathscr{A}_n}$$

称为公式$\mathscr{A}$的**代入实例**(substitute instance).

定理 22.4.2 永真式的任意代入实例必为普效公式.

定理 22.4.3 DeMorgan 律在谓词逻辑中成立.

事实上,在谓词逻辑中的 DeMorgan 律:

$$\neg(\wedge_{i=1}^{n}\mathscr{A}_i)\leftrightarrow\vee_{i=1}^{n}(\neg\mathscr{A}_i),$$

$$\neg(\vee_{i=1}^{n}\mathscr{A}_i)\leftrightarrow\wedge_{i=1}^{n}(\neg\mathscr{A}_i).$$

其中$\mathscr{A}_i(1\leqslant i\leqslant n)$是谓词公式.它是命题逻辑中永真式:

$$\neg(\wedge_{i=1}^{n}P_i)\leftrightarrow\vee_{i=1}^{n}(\neg\mathscr{A}_i),$$

$$\neg(\vee_{i=1}^{n}P_i)\leftrightarrow\wedge_{i=1}^{n}(\neg P_i),$$

的代入实例.

DeMorgan 律还可以推广为带量词的形式

$$\neg(\forall x)\mathscr{A}(x)\leftrightarrow(\exists x)\neg\mathscr{A}(x),$$
$$\neg(\exists x)\mathscr{A}(x)\leftrightarrow(\forall x)\neg\mathscr{A}(x).$$

现在对于带自由变元的公式，对变元作“代入”的问题仔细考虑.

对于谓词公式，经常写作 $\mathscr{A}(x_{i_1},\cdots,x_{i_k})$，这时我们暗示谓词公式 $\mathscr{A}$ 中有自由变元$x_{i_1},\cdots,x_{i_k}$，但是它并不表示公式 $\mathscr{A}$ 中仅有这些自由变元，事实上，公式 $\mathscr{A}$ 中还可以包含其他的变元. 当对这些变元的项 $t_1,\cdots,t_k$ 作代入时，所得的结果 $\mathscr{A}^{t_1,\cdots,t_k}_{x_{i_1},\cdots,x_{i_k}}$ 常简记作 $\mathscr{A}(t_1,\cdots,t_k)$.

定义 22.4.4 设 $\mathscr{A}(x_i)$是合式公式，t 是任意的项，x_j 是 t 中的变元，若 x_i 不自由出现在公式 $\mathscr{A}(x_i)$ 中量词$(\forall x_j)$(或$(\exists x_j)$)的辖域中，则称项 t **对$\mathscr{A}(x_i)$中的x_i 是自由的**(free for x_i in $\mathscr{A}$).

简言之，这时项 t 可以代入 $\mathscr{A}(x_i)$中 x_i 的每一个自由出现，而不会引起 $\mathscr{A}$ 中量词的任何相互作用，产生变元混淆，改变公式的含义.

例 22.4.5 设公式 $P(x_i)$与 $Q(x_1,x_2)$.

(1) 设项 $t=x_j$，则 t 对公式 $P(x_i)$中的 x_i 是自由的(因为公式 $P(x_i)$中无量词).

但是 t 对公式$(\forall x_j)P(x_i)$中的 x_i 是不自由的(因为公式$(\forall x_j)P(x_i)$中的 x_i 在公式中量词$(\forall x_j)$的辖域内).

(2) 设项 $t=f(x_1,x_3)$，则 t 对于公式$(\forall x_2)Q(x_1,x_2)\to P(x_1)$中的 x_1 是自由的. 而 t 对于公式$(\exists x_3)(\forall x_2)Q(x_1,x_2)\to P(x_1)$中的 x_1 是不自由的.

(3) 任意闭项(不含变元的项)对于任意公式中的任意变量都是自由的.

(4) 若 t 中的变元在公式 $\mathscr{A}$ 中不受量词的约束，项 t 对 $\mathscr{A}$ 中任何变元都是自由的.

(5) 变元 x_i 对任意公式中的 x_i 都是自由的.

(6) 若变元 x_i 不在公式 $\mathscr{A}$ 中自由出现,则任意项对 $\mathscr{A}$ 中的 x_i 是自由的.

通过上例可知,检查项 t 对公式 $\mathscr{A}$ 中的变元 x_i 是否自由,可分两步进行:

(1) 查明公式 $\mathscr{A}$ 中的变元 x_i 位于哪些量词 $(\forall y)$(或 $(\exists y)$)的辖域内.

(2) 这些变元 y 是否出现在项 t 中(即是项 t 的变量).

现在把谓词公式(命题函数)的等值式及蕴含式集中陈述如下.

定理 22.4.6 设 x,y 是不同的变元;$\mathscr{A},\mathscr{B},\mathscr{P},\mathscr{A}(x),\mathscr{B}(x),\mathscr{P}(x),\mathscr{P}$ 为公式;$\mathscr{A},\mathscr{B}$ 不含自由变元,则有:

(1) 量词互换律(对偶律)

1) $\neg(\forall x)\mathscr{P}(x) \Leftrightarrow (\exists x)\neg\mathscr{P}(x)$.

2) $\neg(\exists x)\mathscr{P}(x) \Leftrightarrow (\forall x)\neg\mathscr{P}(x)$.

(2) 量词辖域的扩张与收缩

3) $(\forall x)(\mathscr{A}(x)\vee\mathscr{B}) \Leftrightarrow (\forall x)\mathscr{A}(x)\vee\mathscr{B}$.

4) $(\forall x)(\mathscr{A}(x)\wedge\mathscr{B}) \Leftrightarrow (\forall x)\mathscr{A}(x)\wedge\mathscr{B}$.

5) $(\exists x)(\mathscr{A}(x)\vee\mathscr{B}) \Leftrightarrow (\exists x)\mathscr{A}(x)\vee\mathscr{B}$.

6) $(\exists x)(\mathscr{A}(x)\wedge\mathscr{B}) \Leftrightarrow (\exists x)\mathscr{A}(x)\wedge\mathscr{B}$.

7) $(\forall x)(\mathscr{A}(x)\rightarrow\mathscr{B}) \Leftrightarrow (\exists x)\mathscr{A}(x)\rightarrow\mathscr{B}$.

8) $(\forall x)(\mathscr{B}\rightarrow\mathscr{A}(x)) \Leftrightarrow \mathscr{B}\rightarrow(\forall x)\mathscr{A}(x)$.

9) $(\exists x)(\mathscr{A}(x)\rightarrow\mathscr{B}) \Leftrightarrow (\forall x)\mathscr{A}(x)\rightarrow\mathscr{B}$.

10) $(\exists x)(\mathscr{B}\rightarrow\mathscr{A}(x)) \Leftrightarrow \mathscr{B}\rightarrow(\exists x)\mathscr{A}(x)$.

(3) 量词的分配律

11) $(\forall x)(\mathscr{A}(x)\wedge\mathscr{B}(x)) \Leftrightarrow (\forall x)\mathscr{A}(x)\wedge(\forall x)\mathscr{B}(x)$.

12) $(\exists x)(\mathscr{A}(x)\vee\mathscr{B}(x)) \Leftrightarrow (\exists x)\mathscr{A}(x)\vee(\exists x)\mathscr{B}(x)$.

13) $(\exists x)(\mathscr{A}(x)\rightarrow\mathscr{B}(x)) \Leftrightarrow (\forall x)\mathscr{A}(x)\rightarrow(\exists x)\mathscr{B}(x)$.

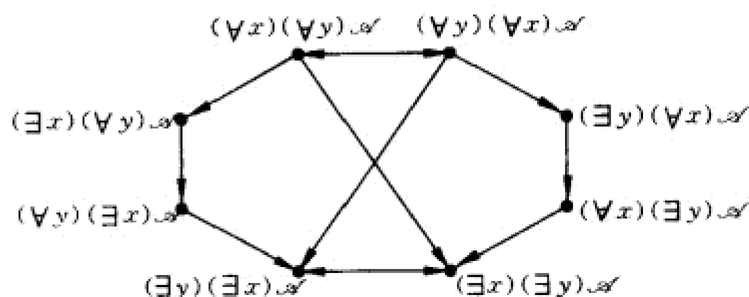


图 22.1

(4) **永真蕴含式**

14) $(\exists x)(\mathscr{A}(x)\wedge\mathscr{B}(x)) \Rightarrow (\exists x)\mathscr{A}(x)\wedge(\exists x)\mathscr{B}(x)$.

15) $(\forall x)\mathscr{A}(x)\vee(\forall x)\mathscr{B}(x) \Rightarrow (\forall x)(\mathscr{A}(x)\vee\mathscr{B}(x))$.

16) $(\exists x)\mathscr{A}(x)\rightarrow(\forall x)\mathscr{B}(x) \Rightarrow (\forall x)(\mathscr{A}(x)\rightarrow\mathscr{B}(x))$.

17) $(\forall x)(\mathscr{A}(x)\rightarrow\mathscr{B}(x)) \Rightarrow (\forall x)\mathscr{A}(x)\rightarrow(\forall x)\mathscr{B}(x)$.

18) $(\forall x)(\mathscr{A}(x)\rightarrow\mathscr{B}(x)) \Rightarrow (\exists x)\mathscr{A}(x)\rightarrow(\exists x)\mathscr{B}(x)$.

19) $(\forall x)(\mathscr{A}(x)\leftrightarrow\mathscr{B}(x)) \Rightarrow (\exists x)\mathscr{A}(x)\leftrightarrow(\exists x)\mathscr{B}(x)$.

20) $(\forall x)(\mathscr{A}(x)\leftrightarrow\mathscr{B}(x)) \Rightarrow (\forall x)\mathscr{A}(x)\leftrightarrow(\forall x)\mathscr{B}(x)$.

注 上述定理是关于单量词的等值式(等价式)与蕴含式.

定理 22.4.7 设 x,y 是不同的变元,$\mathscr{P}(x,y)$是公式,且 x 对 $\mathscr{P}(x,y)$中的 y 是自由的,则有:

(1) 等值式

1) $(\forall x)(\forall y)\mathscr{P}(x,y) \Leftrightarrow (\forall y)(\forall x)\mathscr{P}(x,y)$.

2) $(\exists x)(\exists y)\mathscr{P}(x,y) \Leftrightarrow (\exists y)(\exists x)\mathscr{P}(x,y)$.

(2) **蕴含式**

3) $(\forall x)(\forall y)\mathscr{P}(x,y) \Rightarrow (\exists x)(\forall y)\mathscr{P}(x,y)$.

4) $(\forall y)(\forall x)\mathscr{P}(x,y) \Rightarrow (\exists y)(\forall x)\mathscr{P}(x,y)$.

5) $(\exists x)(\forall y)\mathscr{P}(x,y) \Rightarrow (\forall y)(\exists x)\mathscr{P}(x,y)$.

6) $(\exists y)(\forall x)\mathscr{P}(x,y) \Rightarrow (\forall x)(\exists y)\mathscr{P}(x,y)$.

7) $(\forall y)(\exists x)\mathscr{P}(x,y) \Rightarrow (\exists y)(\exists x)\mathscr{P}(x,y)$.

8) $(\forall x)(\exists y)\mathscr{P}(x,y) \Rightarrow (\exists x)(\exists y)\mathscr{P}(x,y)$.

注 从上述定理可知,同类量词是可以交换的(如(1),(2)).但是不同类量词一般是不可以交换的,现给出示意图 22.1,其中双向箭头标示出等值式,而单向箭头标示出蕴含式.

22.5 谓词逻辑的推理系统

作为命题逻辑的扩充,谓词逻辑的推理系统也可分成自然推理系统与公理推理系统两种类型,本节介绍一种典型的公理推理系统 $K_{\mathscr{L}}$,它是命题逻辑推理系统 L 的扩充.

22.5.1 一阶理论 $K_{\mathscr{L}}$ (K)

一般而言 $K_{\mathscr{L}}$ 是由一个形式语言 $\mathscr{L}$ 的符号库(Alp)($\mathscr{L}$)、合式公式集(由项集 Term($\mathscr{L}$)及公式集 Form ($\mathscr{L}$)组成)、公理集 Axiom ($\mathscr{L}$)以及推理规则集 Rule ($\mathscr{L}$)构成.

定义 22.5.1 (Alp)($\mathscr{L}$) 符号库由下列符号组成:

(1) $x_1, x_2, \cdots$ (变元符号)

(2) $\neg, \rightarrow$ (逻辑联结词)

(3) $\forall$ (全称量词符)

(4) $\neq, =$ (等词符号)

(5)),((括号)

(6) 参数符号包括

1) 谓词符号,

2) 函数符号,

3) 常数(元)符号.

定义 22.5.2 Term($\mathscr{L}$)项集由下列元素组成:

(1) 变元是项;

(2) 常元是项；

(3) f 是 n 元函数符号，$t_1,\cdots,t_n$ 是项，则 $f(t_1,\cdots,t_n)$ 也是项；

(4) 所有的项，均由(1)，(2)，(3) 产生.

定义 22.5.3 Form ($\mathscr{L}$)公式集由下列元素组成：

(1) 设 t_1,t_2 是项，则 $t_1=t_2$ 是公式；

(2) 设 $t_1,\cdots,t_n$ 是项，R 是 n 元谓词符号，则 $R(t_1,\cdots,t_n)$ 是公式；

(3) 若 $\mathscr{A}$ 是公式，则 $\neg\mathscr{A}$ 也是公式；

(4) 若 $\mathscr{A},\mathscr{B}$ 是公式，则 $\mathscr{A}\rightarrow\mathscr{B}$ 是公式；

(5) 若 $\mathscr{A}$ 是公式，x 是变元，则 $(\forall x)\mathscr{A}$ 是公式.

定义 22.5.4 Axiom ($\mathscr{L}$)公理集由下列公理模式组成(参见定义 21.7.1)：

A1 $\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{A})$；

A2 $(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))\rightarrow((\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow\mathscr{C}))$；

A3 $(\neg\mathscr{B}\rightarrow\neg\mathscr{A})\rightarrow((\neg\mathscr{B}\rightarrow\mathscr{A})\rightarrow\mathscr{B})$；

A4 $(\forall x)\mathscr{A}\rightarrow\mathscr{A}$，设 x 在 $\mathscr{A}$ 中不自由出现；

A5 $(\forall x)\mathscr{A}(x)\rightarrow\mathscr{A}(t)$，其中，$\mathscr{A}(x)$ 是 $K_{\mathscr{L}}$ 的公式，而 t 是 $K_{\mathscr{L}}$ 的项在 $\mathscr{A}(x)$ 中关于 x 是自由的；

(注意：由此公理模式明显地有：$(\forall x)\mathscr{A}(x)\rightarrow\mathscr{A}(x)$.)

A6 $(\forall x)(\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow(\forall x)\mathscr{B})$，其中 $\mathscr{A}$ 是 $K_{\mathscr{L}}$ 的公式，x 在 $\mathscr{A}$ 中不自由出现.

以上 A1～A6 是逻辑公理，它包括 L 的公理模式. 此外对于不同的一阶理论还可以有特殊公理模式.

定义 22.5.5 Rule($\mathscr{L}$) 推理(推演)规则集，由下列规则组成(参见定义 21.7.1)：

(1) **分离规则**(modus ponens，MP 规则)：若 $\mathscr{A}$ 且 $\mathscr{A}\rightarrow\mathscr{B}$，则 $\mathscr{B}$ (即 $\vdash\mathscr{A}$，$\vdash\mathscr{A}\rightarrow\mathscr{B}$，则 $\vdash\mathscr{B}$).

(2) **概括规则**(generalization,GEN 规则):若 $\mathscr{A}$,则$(\forall x)\mathscr{A}$(即 $\vdash\mathscr{A}$,则 $\vdash(\forall x)\mathscr{A}$).

注 (1) 在系统 $K_{\mathscr{L}}$ 中,推理规则集中仅有两条推演规则,这些规则是具有“保真性的”,即从普效公式推演出普效公式.

(2) 有些文献中使用的推演规则要多一些,最常见的是给出有关量词的 4 条重要性质作为推演规则:

1) **全称特指规则**(universal specification,US):$(\forall x)\mathscr{A}(x)\Rightarrow\mathscr{A}(t)$,$t$ 是项.

2) **全称推广规则**(universal generalization,UG):$\mathscr{A}(x)\Rightarrow(\forall x)\mathscr{A}(x)$,$x$ 不在前提 $\mathscr{A}(x)$中自由出现.

3) **存在特指规则**(existential specification,ES):$(\exists x)\mathscr{A}(x)\Rightarrow\mathscr{A}(c)$,$c$ 是常元.

4) **存在推广规则**(existential generalization,EG):$\mathscr{A}(c)\Rightarrow(\exists x)\mathscr{A}cx$,$c$ 是常元.

事实上,US 就是系统 $K_{\mathscr{L}}$ 中的公理 A5,UG 就是 $K_{\mathscr{L}}$ 中的推演规则 GEN,EG 是从普效式 $\vdash\mathscr{A}(x)\to(\exists x)\mathscr{A}(x)$转化而来,ES 是一种极为常用的推演规则.

下面是推演(证明)的例子.

例 22.5.6 $(\forall x)(\mathscr{M}(x)\to\mathscr{F}(x)),(\forall x)(\mathscr{K}(x)\to\mathscr{M}(x))\vdash(\forall x)(\mathscr{K}(x)\to\mathscr{F}(x))$.

证明

(1) $(\forall x)(\mathscr{M}(x)\to\mathscr{F}(x))$; 假设

(2) $\mathscr{M}(c)\to\mathscr{F}(c)$; (1) US

(3) $(\forall x)(\mathscr{K}(x)\to\mathscr{M}(x))$; 假设

(4) $\mathscr{K}(c)\to\mathscr{M}(c)$; (3) US

(5) $\mathscr{K}(c)\to\mathscr{F}(c)$; (2),(4) MP

(6) $(\forall x)(\mathscr{K}(x)\to\mathscr{F}(x))$. (5) UG

例 22.5.7 $(\forall x)(\mathscr{L}(x)\to\mathscr{D}(x)),(\exists x)\mathscr{L}(x)\vdash(\exists x)\mathscr{D}(x)$.

证明

(1) $(\exists x)\mathscr{L}(x)$;　　　　假设

(2) $\mathscr{L}(a)$;　　　　(1) ES

(3) $(\forall x)(\mathscr{L}(x)\rightarrow\mathscr{D}(x))$;　　　　假设

(4) $\mathscr{L}(a)\rightarrow\mathscr{D}(a)$;　　　　(3) US

(5) $\mathscr{D}(a)$;　　　　(2),(4) MP

(6) $(\exists x)\mathscr{D}(x)$.　　　　(5) EG

例 22.5.8　偏序理论

该理论 $K_{\mathscr{Y}}$ 仅有一个谓词$<(x,y)$,即"x 小于 y",则有两条特殊公理:

(1) $(\forall x)(x \not< x)$;　　　　(非自反性)

(2) $(\forall x)(\forall y)(\forall z)((x<y)\wedge(y<z)\rightarrow(x<z))$.

(传递性)

这个理论的模型称为偏序集.

例 22.5.9　群理论

设 K 有一个谓词符号$=(t,s)$(即 $t=s$,是等符),一个函数符号 $f(t,s)=t+s$(即 f 是"加法"运算),一个常元符号 0(即"加法"单元),这时的特殊公理是:

(1) $(\forall x)(\forall y)(\forall z)(x+(y+z)=(x+y)+z)$;(结合律)

(2) $(\forall x)(0+x=x)$;　　　　(单元存在性)

(3) $(\forall x)(\exists y)(y+x=0)$;　　　　(逆元存在性)

(4) $(\forall x)(x=x)$;　　　　(自反性)

(5) $(\forall x)(\forall y)(x=y\rightarrow y=x)$;　　　　(对称性)

(6) $(\forall x)(\forall y)(\forall z)(x=y\rightarrow(y=z\rightarrow x=z))$;　　　　(传递性)

(7) $(\forall x)(\forall y)(\forall z)(y=z\rightarrow(x+y=x+z\wedge y+x=z+x))$.

这个理论的模型就是群.

从上述例子可知,偏序理论与群理论都是可公理化的理论.

22.5.2 一阶理论的性质

一阶理论是命题逻辑的扩充，因此有关系统 K 中的证明、推演以及定理诸概念，都可经适当地扩充后，移植过来.

定义 22.5.10(参见定义 21.7.2)

(1) 设 Γ 是系统 K 中的公式集，$\mathscr{A}\in\Gamma$，若存在 K 中的公式序列：$\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_n$ 满足下列条件之一：

1) $\mathscr{A}_n=\mathscr{A}$;

2) $\mathscr{A}_i(1\leqslant i\leqslant n)$ 是 K 中的公理；

或 3) $\mathscr{A}_i\in\Gamma,(1\leqslant i\leqslant n)$；

或 4) $\mathscr{A}_i(1\leqslant i\leqslant n)$ 是序列中较前的两个公式应用推理规则 MP 或 GEN 后的直接推论.

则称 $\mathscr{A}$ 是 Γ 的**推论(后承)**(consequence)，记作 $\Gamma\vdash_K\mathscr{A}$.

(2) 定义(1) 中的序列：$\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_n$ 称为 $\mathscr{A}(\mathscr{A}=\mathscr{A}_n)$ 从 Γ 的**证明(推演)**(proof/deduction)，Γ 称作证明的**假设**(hypothese)或**前提**(premise).

(3) 当 Γ 是空集 $\varnothing$ 时，则记号 $\varnothing\vdash_K\mathscr{A}$ 简记为 $\vdash_K\mathscr{A}$，称公式 $\mathscr{A}$ 是 K 中的**定理**(theorem)或**可证公式**(provable formula).

定理 22.5.11 公理模式 A1～A6 的代入实例都是普效公式.

定理 22.5.12 K 的可靠性定理 设 $\mathscr{A}\in$ Form($\mathscr{L}$)，若 $\vdash_K\mathscr{A}$，则 $\models\mathscr{A}$.

定理 22.5.13 K 的古典相容性定理

K 是相容的(不存在任何公式 $\mathscr{A}$ 使得 $\vdash_K\mathscr{A}$ 且 $\vdash_K\neg\mathscr{A}$)(参看定义 22.7.12).

注 对于 K 中的任意公式 $\mathscr{A}$，有 $\mathscr{A}\vdash_K(\forall x)\mathscr{A}$，但是 $\vdash_K(\mathscr{A}\rightarrow(\forall x)\mathscr{A})$ 却未必成立.

定理 22.5.14 K 的演绎定理 设 $\mathscr{A},\mathscr{B}\in$ Form($\mathscr{L}$)，Γ 是 $\mathscr{L}$

中的公式集(可能是空集). 若 $\Gamma\cup\{\mathscr{A}\}\vdash_K\mathscr{B}$,并且推演对涉及 $\mathscr{A}$ 中自由出现的变元没有使用过 GEN 规则,则有 $\Gamma\vdash_K(\mathscr{A}\to\mathscr{B})$(参考定理 21.7.7).

K 的演绎定理较之 L 的演绎定理复杂,这是由于在谓词演算系统中,公式 $\mathscr{A}$ 中含有自由变元的缘故.

定理 22.5.15 若 $\Gamma\cup\{\mathscr{A}\}\vdash_K\mathscr{B}$,并且 $\mathscr{A}$ 是一闭公式,则 $\Gamma\vdash_K(\mathscr{A}\to\mathscr{B})$.

定理 22.5.16 **假言三段论规则** (HS)(参见定理 21.7.9) 对任意公式 $\mathscr{A},\mathscr{B},\mathscr{C}\in\mathrm{Form}(\mathscr{L})$有$\{(\mathscr{A}\to\mathscr{B}),(\mathscr{B}\to\mathscr{C})\}\vdash_K(\mathscr{A}\to\mathscr{C})$.

定理 22.5.17 **演绎定理的逆定理** (参见定理 21.7.8) 设 $\mathscr{A},\mathscr{B}\in\mathrm{Form}(\mathscr{L})$,$\Gamma$ 是公式集. 若 $\Gamma\vdash_K(\mathscr{A}\to\mathscr{B})$,则 $\Gamma\cup\{\mathscr{A}\}\vdash_K\mathscr{B}$.

定理 22.5.18 设 $\mathscr{A},\mathscr{B}\in\mathrm{Form}(\mathscr{L})$,则有 $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{B})\Leftrightarrow\ \vdash_K(\mathscr{A}\to\mathscr{B})$,并且 $\vdash_K(\mathscr{B}\to\mathscr{A})$.

定义 22.5.19 若 $\mathscr{A},\mathscr{B}\in\mathrm{Form}(\mathscr{L})$,且 $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{B})$,则称公式 $\mathscr{A},\mathscr{B}$ 是**等值的**(**等价的**)(equivalent)

显然公式 $\mathscr{A},\mathscr{B}$ 间的等值关系是一种等价关系.

定理 22.5.20 设 $\mathscr{A},\mathscr{B},\mathscr{C}\in\mathrm{Form}(\mathscr{L})$,若 $\mathscr{A}$ 和 $\mathscr{B}$ 是等值的,并且 $\mathscr{B}$ 和 $\mathscr{C}$ 是等值的,则 $\mathscr{A}$ 和 $\mathscr{C}$ 也是等值的.

定理 22.5.21 若变元 x 在 $\mathscr{A}(x)$中自由出现,而 y 是不在 $\mathscr{A}(x)$ 中出现的变元,则有

$$\vdash((\exists x)\mathscr{A}(x)\leftrightarrow(\exists y)\mathscr{A}(y)),$$

$$\vdash_K((\forall x)\mathscr{A}(x)\leftrightarrow(\forall y)\mathscr{A}(y)).$$

定理 22.5.21 表明,可以对一个约束变元进行换名,换名后得到的公式与原公式是证明上等值的公式. 实际上,它说明在系统 K 中约束变元的换名规则也是成立的.

定理 22.5.22 设 $\mathscr{A}\in\mathrm{Form}(\mathscr{L})$,$x_1,\cdots,x_n$ 是 $\mathscr{A}$ 中的自由变元,则 $\vdash_K\mathscr{A}$ 的充要条件是

$\vdash_K (\forall x_1)(\forall x_2)\cdots(\forall x_n)\mathscr{A}$.

定义 22.5.23 若 $\mathscr{A}\in \mathrm{Form}(\mathscr{L})$，$x_1,\cdots,x_n$ 是 $\mathscr{A}$ 中仅有的自由变元，则公式 $(\forall x_1)(\forall x_2)\cdots(\forall x_n)\mathscr{A}$ 称为公式 $\mathscr{A}$ 的**全称闭包**(universal closure)．记作 $\mathscr{A}'$.

注 上述定理说明，对于任意的公式 $\mathscr{A}\in \mathrm{Form}(\mathscr{L})$，$\vdash_K\mathscr{A}$ 的充要条件是 $\vdash_K\mathscr{A}'$；但一般情况下公式 $\mathscr{A}$，$\mathscr{A}'$ 不一定是等价的，因为 $\vdash_K(\mathscr{A}'\to\mathscr{A})$ 虽然总是成立的，但 $\vdash_K(\mathscr{A}\to\mathscr{A}')$ 却不一定成立.

22.5.3 完全性定理

在系统 K 中 Gödel 完全性定理如下.

定理 22.5.24 *K* 的语义完全性 若公式 $\mathscr{A}\in \mathrm{Form}(\mathscr{L})$ 是一个普效公式，则 $\mathscr{A}$ 是 K 中的定理．简记作 $\models\mathscr{A}\Rightarrow\ \vdash_K\mathscr{A}$（参见定理 22.5.12）.

注 (1) 定理 22.5.24 是 Gödel 于 1930 年首次给出的，由于它的重要性，人们常称为 **Gödel 完全性定理.**

(2) 有些文献中把定理 22.5.24 与定理 22.5.12 组合起来得出下述形式的定理：

若公式 $\mathscr{A}\in \mathrm{Form}(\mathscr{L})$，则 $\models\mathscr{A}\Leftrightarrow\ \vdash_K\mathscr{A}$. 称它为 Gödel 完全性定理.

由此定理表明谓词逻辑与命题逻辑一样，在纯形式的语法研究与语义研究之间是可以互相沟通的，K 中的定理恰好是逻辑普效式，谓词逻辑之所以如此重要和有用就在于它有这种性质.

(3) 由于 Gödel 完全性定理的重要，Hilbert 与 Ackermann 于 1938 年，Henkin，L. 于 1949 年，Hasenjaegor，G. 于 1953 年给出了各种不同的证明.

22.5.4 前束范式

命题逻辑中有范式的概念，谓词逻辑中则有前束范式的概念.

命题逻辑中，公式和它的范式都是等值的(等价的). 但是谓词逻辑中，公式和它的各种范式，有些是等值的(等价的)，有些却不是等值的而是可互推的(可以互相推演的).

定义 22.5.25 一阶理论中的公式，具有如下的形式，称为**前束范式**(prenex normal form).

$$(Q_1x_1)\cdots(Q_nx_n)\mathscr{A}.$$

其中 $Q_i(1\leqslant i\leqslant n)$为量词∀或∃，$\mathscr{A}$为不含量词的公式.

(**注** 有些文献中把 $\mathscr{A}$ 为析取范式或合取范式时，称为前束范式，其余情形称为前束形式，本书不作这样的区分.)

定理 22.5.26 前束范式存在定理 一阶理论中任意的公式，必有与之等值(等价)的前束范式.

算法 22.5.27 求前束范式的算法 执行步骤如下：

(1) 约束变元换名. 把公式中的约束变元进行换名，使得每个量词所约束的变元彼此不同，并与公式中的自由变元也不相同(见定理 22.5.21).

(2) 消去量词前面的否定词. 把位于量词前面(左边)的否定词，移到量词的后面(右边)(见定理 22.4.6).

(3) 量词前移. 把公式中的量词逐个移到公式的前面(左边)，最后形成如下的形式：$(Q_1x_1)\cdots(Q_nx_n)\mathscr{B}$，就是前束范式(参见定理 22.4.6).

由于公式 $\mathscr{A}$ 是有穷长的符号串，经有限步后必定终止.

例 22.5.28 求公式$(\forall x)\mathscr{A}(x)\to(\exists x)\mathscr{B}(x)$的前束范式.

解 利用定理 22.4.6 求前束范式如下：

$(\forall x)\mathscr{A}(x)\to(\exists x)\mathscr{B}(x)$

$\Leftrightarrow\neg((\forall x)\mathscr{A}(x))\vee(\exists x)\mathscr{B}(x)$

$\Leftrightarrow(\exists x)(\neg\mathscr{A}(x))\vee(\exists x)\mathscr{B}(x)$

$\Leftrightarrow(\exists x)(\neg\mathscr{A}(x)\vee\mathscr{B}(x))$.

例 22.5.29 求公式$(\forall x)(\forall y)((\exists z)(\mathscr{A}(x,z)\wedge\mathscr{A}(y,z)))$

$\rightarrow (\exists u)\mathscr{B}(x,y,u)$的前束范式.

解 利用定理 22.4.6,求前束范式如下:

$$(\forall x)(\forall y)((\exists z)(\mathscr{A}(x,z) \wedge \mathscr{A}(y,z))) \rightarrow (\exists u)\mathscr{B}(x,y,u)$$
$$\Leftrightarrow (\forall x)(\forall y)(\neg((\exists z)(\mathscr{A}(x,z) \wedge \mathscr{A}(y,z))) \vee (\exists u)\mathscr{B}(x,y,u))$$
$$\Leftrightarrow (\forall x)(\forall y)(\forall z)(\neg \mathscr{A}(x,z) \vee \neg \mathscr{A}(y,z)) \vee (\exists u)\mathscr{B}(x,y,u))$$
$$\Leftrightarrow (\forall x)(\forall y)(\forall z)(\exists u)(\neg \mathscr{A}(x,z) \vee \neg \mathscr{A}(y,z) \vee \mathscr{B}(x,y,u)).$$

例 22.5.30 求公式 $\mathscr{A}(x,y) \rightarrow (\exists y)[\mathscr{B}(y) \rightarrow (((\exists x)\mathscr{B}(x)) \rightarrow \mathscr{C}(y))]$的前束范式.

解

$$\mathscr{A}(x,y) \rightarrow (\exists y)[\mathscr{B}(y) \rightarrow (((\exists x)\mathscr{B}(x)) \rightarrow \mathscr{C}(y))]$$
$$\Leftrightarrow \mathscr{A}(x,y) \rightarrow (\exists y)[\mathscr{B}(y) \rightarrow (\forall u)(\mathscr{B}(u) \rightarrow \mathscr{C}(y))]$$
$$\Leftrightarrow \mathscr{A}(x,y) \rightarrow (\exists y)(\forall v)(\mathscr{B}(y) \rightarrow (\mathscr{B}(u) \rightarrow \mathscr{C}(y)))$$
$$\Leftrightarrow (\exists w)(\mathscr{A}(x,y) \rightarrow (\forall v)(\mathscr{B}(w) \rightarrow (\mathscr{B}(v) \rightarrow \mathscr{C}(w))))$$
$$\Leftrightarrow (\exists w)(\forall z)(\mathscr{A}(x,y) \rightarrow (\mathscr{B}(w) \rightarrow (\mathscr{B}(z) \rightarrow \mathscr{C}(w)))).$$

例 22.5.31 求公式 $(\exists x)(\forall u)((\mathscr{A}(u,v) \rightarrow \neg \mathscr{B}(x)) \rightarrow (\forall y)(\forall z)\mathscr{C}(y,z))$的前束范式.

解 下述两公式都是所求的前束范式:

$(\exists x)(\forall u)(\forall y)(\forall z)((\mathscr{A}(u,v) \rightarrow \neg \mathscr{B}(x)) \rightarrow \mathscr{C}(y,z))$;

$(\forall y)(\forall z)(\forall u)(\exists x)((\mathscr{A}(u,v) \rightarrow \neg \mathscr{B}(x)) \rightarrow \mathscr{C}(y,z))$.

注 算法 22.5.27 并不导致唯一的解答,一般情形,与一个公式等值的前束范式会有多个(参见例 22.5.31).

由上述诸例可以看出,在前束范式中其前面的量词既有全称量词,也有存在量词,由前面可知,同类型(如同为全称量词)的量词是可以交换次序的,但不同类型的量一般是不可以随便交换的.

定义 22.5.32 满足下述条件的前束范式,称为 **∃-前束范式**(∃-prenex normal form)或 Skolem **范式**(Skolem normal form).

(1) ∃-前束范式是前束范式;

(2) ∃-前束范式是闭公式(其中无自由变元);

(3) 公式中至少有一个存在量词;

(4) 公式中一切存在量词都在全称量词之前.

定理 22.5.33 ∃-前束范式存在定理 设 $\mathscr{A}$ 是纯谓词演算中的公式,则必有∃-前束范式 $\mathscr{B}$ 使得 $\vdash\mathscr{A}$ 的充要条件是 $\vdash\mathscr{B}$.

注 无函数符号或常元符号的一阶理论,常称为**纯谓词演算**(predicate calculus).

例 22.5.34 判断下列公式是否是∃-前束范式.

(1) $(\exists x)(\forall y)(\mathscr{A}(x,y)\wedge\mathscr{B}(x,y,z))$;

(2) $(\forall x)(\mathscr{A}(x)\to\mathscr{B}(x))$;

(3) $(\exists x)(\forall y)(\mathscr{A}(x)\to\mathscr{C}(x,y))$.

解

(1) 的公式中含有自由变元 z,所以它不是∃-前束范式. (2) 的公式中缺少存在量词,它也不是∃-前束范式. (3) 是闭公式,其中无自由变元,且有存在量词,而存在量词又在全称量词之前,所以它是∃-前束范式.

算法 22.5.35 计算∃-前束范式的算法 执行步骤如下:

(1) 设 $\mathscr{A}$ 是前束范式,含有自由变元 $x_1,\cdots,x_n$(注意这时 $\mathscr{A}$ 中还可能含有其他的约束变元),求公式 $\mathscr{A}$ 的闭包 $\mathscr{A}'$.

$$\mathscr{A}'=(\forall x_1)\cdots(\forall x_n)\mathscr{A},$$

对 $\mathscr{A}'$ 执行(2).

(2) 1)若 $\mathscr{A}'$ 为不含∃量词的闭式,亦即 $\mathscr{A}$ 中不含∃量词,则引入在 $\mathscr{A}'$ 中不出现的一元谓词 $P(\cdot)$,在 $\mathscr{A}'$ 中不出现的个体变元 y,构造一个新的前束范式:$(\exists y)(\mathscr{A}'\wedge(P(y)\vee\neg P(y)))$,再把 $\mathscr{A}'$ 代入,即得 $(\exists y)((\forall x_1)\cdots(\forall x_n)\mathscr{A}\wedge(P(y)\vee\neg P(y)))$,也就是 $(\exists y)(\forall x_1)\cdots(\forall x_n)(\mathscr{A}\wedge(P(y)\vee\neg P(y)))$,这就是所求的∃-前束范式.

2)若 $\mathscr{A}'$ 中含有∃量词,亦即 $\mathscr{A}$ 中含有∃量词,设 $\mathscr{A}$ 的形式如下:
$(\exists x_1)\cdots(\exists x_i)(\forall x_{i+1})\mathscr{B}(x_1,\cdots,x_{i+1})\quad(i\geqslant 1)$,$\mathscr{B}$ 中的自

由变元是 $x_1,\cdots,x_{i+1}$. 若 $\mathscr{B}$ 中再无存在量词,则上式即为所求. 若 $\mathscr{B}$ 中仍含有存在量词,则按下述方法把 $(\forall x_{i+1})$ 归约为 $(\exists x_{i+1})(\forall v)$: 引入一个在 $\mathscr{B}$ 中不出现的 $(i+1)$ 元谓词 R 以及在 $\mathscr{B}$ 中不出现的变元 v,把下式

$$(\exists x_1)\cdots(\exists x_i)(\forall x_{i+1})\mathscr{B}(x_1,\cdots,x_{i+1})$$

变为

$(\exists x_1)\cdots(\exists x_i)((\exists x_{i+1})\mathscr{B}(x_1,\cdots,x_{i+1})\wedge\neg R(x_1,\cdots,x_{i+1}))\vee(\forall v)R(x_1,\cdots,x_i,v)$,

或 $(\exists x_1)\cdots(\exists x_i)(\exists x_{i+1})(\forall v)((\mathscr{B}(x_1,\cdots,x_{i+1})\wedge\neg R(x_1,\cdots,x_{i+1}))\vee R(x_1,\cdots,x_i,v))$,

或 $(\exists x_1)\cdots(\exists x_i)(\exists x_{i+1})(\forall v)((\mathscr{B}(x_1,\cdots,x_{i+1})\rightarrow R(x_1,\cdots,x_{i+1}))\rightarrow R(x_1,\cdots,x_i,v))$,

若此时 $\mathscr{B}$ 中再无存在量词,则该式即为所求. 否则,把公式记为:

$$(\exists x_1)\cdots(\exists x_{i+1})(\forall v)\mathscr{C}(x_1,\cdots,x_i,v).$$

再按 $\mathscr{C}$ 中有无存在量词进行讨论,重复执行上述算法.

例 22.5.36 求公式 $(\exists x)(\forall y)(\exists u)R(x,y,u)$ 的 $\exists$-前束范式.

解 记 $\mathscr{B}(x,y)=(\exists u)R(x,y,u)$,依算法 22.5.27 将原式记作 $(\exists x)(\forall y)\mathscr{B}(x,y)$.

现引入一个在 $\mathscr{B}$ 中不出现的二元谓词 S 以及在 $\mathscr{B}$ 中不出现的变元 z,则由算法 22.5.27 可知原式变为

$(\exists x)(\exists y)((\mathscr{B}(x,y)\wedge\neg S(x,y))\vee(\forall z)S(x,z))$.

将 $\mathscr{B}(x,y)$ 代入

$(\exists x)(\exists y)(((\exists u)R(x,y,u)\wedge\neg S(x,y))\vee(\forall z)S(x,z))$,

将 $(\exists y)(\exists u)$ 前移

$(\exists x)(\exists y)(\exists u)((R(x,y,u)\wedge\neg S(x,y))\vee(\forall z)S(x,z))$,

再把 $(\forall z)$ 前移

$(\exists x)(\exists y)(\exists u)(\forall z)((R(x,y,u)\wedge\neg S(x,y))\vee S(x,z))$,

这就是 $\exists$-前束范式.

例 22.5.37 求公式$(\forall x)(\exists y)\mathscr{A}(x,y)$的 Skolem 范式 $\mathscr{B}$，并且证明 $\nvdash \mathscr{B}\leftrightarrow(\forall x)(\exists y)\mathscr{A}(x,y)$.

解 公式$(\forall x)(\exists y)\mathscr{A}(x,y)$的 Skolem 范式 $\mathscr{B}$ 为

$$\mathscr{B}=(\exists x)(\exists y)(\forall z)([\mathscr{A}(x,y)\to\mathscr{C}(x)]\to\mathscr{C}(z)).$$

为了证明 $\nvdash \mathscr{B}\leftrightarrow(\forall x)(\exists y)\mathscr{A}(x,y)$. 只要在论域 $I=\{1,2\}$ 中，把谓词 $\mathscr{A}(x,y)$ 解释为"$x<y$"，谓词 $\mathscr{C}(u)$ 解释为"$u=2$"就行了.

由例 22.5.37 可知，在谓词演算中一个公式的 Skolem 范式与原公式之间仅有互推(互相推演)的关系，两者并不逻辑等值(等价).

22.5.5 带等词的一阶理论

"相等"概念在许多数学理论和程序理论中都是必不可少的重要概念. 可以通过引入"等词"或"等号"所表示的谓词来构成用语言 $K_{\mathscr{L}}$ 表达的一阶理论.

首先给出相等公理的定义.

定义 22.5.38 下列公理模式称为**相等公理**(axiom of equality).

E1 $x=x$.

E2 $(t_k=u)\to f(t_1,\cdots,t_k,\cdots,t_n)=f(t_1,\cdots,u,\cdots,t_n)$,

其中 $t_1,\cdots,t_n,u$ 是任意项，f 是 $\mathscr{L}$ 中的函数符号.

E3 $(t_k=u)\to(R(t_1,\cdots,t_k,\cdots,t_n)\to R(t_1,\cdots,u,\cdots,t_n))$,

其中 $t_1,\cdots,t_n,u$ 是任意项，R 是 $\mathscr{L}$ 中的谓词符号.

注 (1) 相等公理模式可以是开公式的形式，也可以是闭公式的形式. 上述定义是开公式的形式，如果对 E1～E3 取它们的全称闭包，就是闭公式的形式，两者在逻辑上是等价的.

(2) 相等公理模式还有一种更为精练的形式：

E1′ $(\forall x)(x=x)$.

E2′ $(x=y)\to(\mathscr{A}(x,x)\to\mathscr{A}(x,y))$，其中 x,y 是变元，

$\mathscr{A}(x,x)$，$\mathscr{A}(x,y)$都是公式.

定义 22.5.39 任何包括公理模式 E1～E3 的 $K_{\mathscr{L}}$ 系统称为**带等号的一阶理论(系统)**(first order theory with equality).

定理 22.5.40 设 $\mathscr{E}$ 是带等号的一阶理论，则有：

(1) $\vdash_{\mathscr{E}}(\forall x)(x=x)$. 自反性

(2) $\vdash_{\mathscr{E}}(\forall x)(\forall y)(x=y\to y=x)$. 对称性

(3) $\vdash_{\mathscr{E}}(\forall x)(\forall y)(\forall z)(x=y\to(y=z\to x=z))$. 传递性

根据定理 22.5.40 可知，相等关系与等价关系一样具有自反性、对称性与传递性，而且在一阶理论的框架内是不可区分的. 这种情况可通过下面的例子看出.

例 22.5.41 设 $x_1,x_2,\cdots$ 是 $\mathscr{L}$ 中的变元，函数符号有加法函数 add(x,y)："$x+y$". 等词："$x=y\triangleq x\equiv y(\mathrm{mod}2)$"；换言之，$x=y$ 的含义是指"x,y 在模 2 同余的关系下相等"，可以证明公理模式 E1～E3 均可满足.

上述例子表明 Z_2(即模 2 同余类)是带等号的一阶理论的一个模型，在这个模型中"等词"被解释成同余相等"$\equiv$"的等价关系(而不是"相等"的关系).

但是我们有下面的定理.

定理 22.5.42 若 $\mathscr{E}$ 是相容的带等号的一阶理论，则 $\mathscr{E}$ 有一个模型(结构)，其中等词的解释是$=$.

对于任何带等号的一阶理论，它有无限多个模型. 上述定理说明在这些模型中必有一个模型，它的等号(等词)被解释为$=$(相等). 因此，我们有下面定义.

定义 22.5.43 带等号的一阶理论 $\mathscr{E}$ 中，等号被解释为$=$的模型，称为 $\mathscr{E}$ 的**标准模型**(normal model).

关于标准模型，有下述重要定理.

定理 22.5.44 任意带等号的相容理论，必有一个有限或可

列(可数)的标准模型.

定理 22.5.45 任意带等号的理论若有一个无穷标准模型，则必有一个可列(可数)标准模型.

下面的例子都是一阶理论.

例 22.5.46 群的初等理论(二阶理论)G.

设等号谓词：$=$

加法函数符号：$f(t,s)$：$t+s$

常元符号：0

G 的特殊公理是：

(1) $x+(y+z)=(x+y)+z$;

(2) $x+0=x$;

(3) $(\forall x)(\exists y)(x+y=0)$;

(4) $x=x$;

(5) $(x=y)\to(y=x)$;

(6) $(x=y)\to(y=z\to x=z)$;

(7) $(x=y)\to(x+z=y+z\wedge z+x=z+y)$;

(8) $x+y=y+x$.

满足公理(1) ～(7) 的是群 G 的一阶理论. 满足公理(1) ～(8) 的是交换群的一阶理论(参见例 22.5.9). 在例 22.5.9 中群的特殊公理是以闭公式的形式给出的.

例 22.5.47 域的一阶理论.

除了群理论中的特殊公理外，对于域的理论还需增加乘法函数 $g(t,s)$：$t\cdot s$ 和乘法单元：1，以及下述公理.

(9) $(x=y)\to(x\cdot z=y\cdot z\wedge z\cdot x=z\cdot y)$;

(10) $(x\cdot y)\cdot z=x\cdot(y\cdot z)$;

(11) $x(y+z)=(x\cdot y)+(x\cdot z)$;

(12) $x\cdot y=y\cdot x$;

(13) $x \cdot 1 = x$;

(14) $(x \neq 0) \to (\exists y)(x \cdot y = 1)$;

(15) $0 \neq 1$.

例 22.5.48 配对理论

在配对理论中，需要增加下列谓词与函数.

atom(x)："x 是原子"

pair(x)："x 是偶对"

$\langle x, y \rangle$："配对函数"

当变元 x 是原子时，atom(x) $= \top$(取"真"值)，当变元 x 是偶对时，atom(x) $= \bot$(取"假"值). 对于谓词 pair(x)，情况类似. 当变元 x, y 均为原子时，配对函数的值就是偶对 $\langle x, y \rangle$.

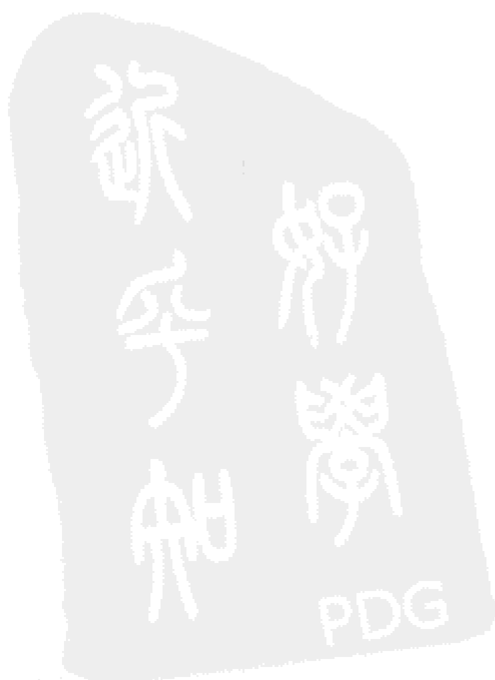
配对理论的特殊公理是：

(1) $(\forall z)[\text{pair}(z) \leftrightarrow (\exists x)(\exists y)(\text{atom}(x) \wedge \text{atom}(y) \wedge (z = \langle x, y \rangle))]$;

(2) $(\forall z)[\neg(\text{atom}(z) \wedge \text{pair}(z))]$;

(3) $(\forall x)(\forall y)(\forall u)(\forall v)[(\text{atom}(x) \wedge \text{atom}(y) \wedge \text{atom}(u) \wedge \text{atom}(v)) \to ((\langle x, y \rangle = \langle u, v \rangle) \to (x = u \wedge y = v))]$.

注 公理(1) 表明偶对的构成；公理(2) 表明变元不可能既是原子，又是偶对；公理(3) 表明偶对的唯一性.



23 非标准(非古典)逻辑

23.1 引言

非标准逻辑,一般泛指与古典命题逻辑和古典谓词逻辑不同的那些逻辑,自古以来早就有之;由于近年来计算机科学与人工智能的发展,使得非标准逻辑的理论与应用都十分活跃.本章将给出一个简略的概述.

非标准逻辑大体上可以划分为两类:一类是与古典逻辑平行的逻辑,如直觉主义逻辑、多值逻辑和模糊逻辑.另一类是对古典逻辑进行扩充的逻辑,如模态逻辑、时态逻辑与动态逻辑.

与古典逻辑平行的非标准逻辑系统所使用的形式语言与古典逻辑的语言基本相同.它们的差别在于古典逻辑系统中的某些定理,在这类逻辑中不再成立(即不再是定理).例如古典逻辑系统中的“排中律”是一条定理,但它在直觉主义逻辑或多值逻辑系统中都是不可证明的.

对古典逻辑进行扩充的非标准逻辑系统中,古典逻辑的定理仍然成立.它们在下述两方面对古典逻辑进行了扩充:

(1) 扩充了古典逻辑的语言;

(2) 补充了古典逻辑的定理.

这是由于这类逻辑系统扩大了古典逻辑系统的词汇表.增加了新的公理和新的算子,因而增强了它们的表达能力,使得那些难以用古典逻辑语言表达的定理推演变得容易了,扩大了古典逻辑的应用领域.

由于非标准逻辑种类繁多,无法逐一介绍,现只介绍模态逻

辑、多值逻辑.

23.2 模态逻辑

模态逻辑是研究包含模态词"必然"与"可能"的模态命题及其推理的逻辑,它对古典逻辑进行了扩充,对命题作了更为细致的刻画. 早在两千多年前,亚里士多德就研究过模态逻辑. 但他的研究不为人们所理解. 直到1880年 H. MacColl 最早使用符号对模态逻辑进行系统地研究,模态逻辑重新得到人们的重视. 然而系统地使用符号与建立模态逻辑系统是从1912年 Lewis 的工作开始,1932年他与 Langford 合著的"Symbolic Logic"书中建立了 Lewis 的模态命题系统 S1～S5. 1933年 K. Gödel 在古典命题逻辑的基础上添加了新公理与新的推演规则,首先给出了模态逻辑的公理化系统. 其后在1937年 Feys 改进了 Gödel 系统建立了系统 T,1951年 Von Wright 又建立了系统 M. 后来知道系统 T 与 M 是等价的. 但在语义方面系统化的结构(框架)语义直到1959年 Kripke 的工作才开始.

23.2.1 模态命题逻辑系统

模态命题逻辑系统是古典命题逻辑系统 L 的扩充. 它是在 L 的基础上加进"必然"与"可能"两个模态算子而构成的.

"必然"与"可能"两个算子,分别用符号$\Box$(或 L),$\Diamond$(或 M)来表示. 对于任何命题 $\mathscr{A}$,有命题

"$\mathscr{A}$ 是必然的",记作$\Box\mathscr{A}$;

"$\mathscr{A}$ 是可能的",记作$\Diamond\mathscr{A}$.

在古典逻辑中,命题有真的或假的.

在模态逻辑中,还要在真命题中区分必然真的和不必然真的(可能真的)命题,在假命题中区分必然假的和不必然假的(可能假

的）命题.

Leibniz 用可能世界的观点来解释“必然”与“可能”. 如果一个命题在所有的可能世界都成立，就称这个命题是“必然的”. 如果一个命题至少在某一个可能世界成立，就称这个命题是“可能的”. 可能世界包括我们能想象的任何世界，例如“虚拟现实”也是一种可能世界. 现实世界也是可能世界中的一个.

因此，从模态逻辑的观点看，命题可分为必然的与偶然的：命题是必然真的，即它在一切可能世界中都为真. 命题是必然假的（命题是不可能真的），即它在一切可能世界中都为假. 命题是偶然真的，即它在某些可能世界是真的，而在另一些可能世界是假的. 命题是偶然假的，即它在某些可能世界是假的，而在另一些可能世界是真的.

必须注意，这里所说的“必然”与“可能”是指逻辑上的必然与可能.

首先给出两个较弱的模态逻辑系统 S1 与 T，在此基础上陆续给出其他的系统，以及它们之间的关系.

定义 23.2.1　系统 S1

(1) **符号(字母)库**

命题字母(statement letter)：$P,Q,R,\cdots,P_1,Q_1,R_1,\cdots,P_2,Q_2,R_2,\cdots$

初始联结词(primitive connective)：$\neg$，$\wedge$.

辅助符号(auxiliary symbol)：括号)，(.

模态算子(modal operator)：$\Diamond(M)$.

(2) **合式公式集(公式集)**

1) 所有的命题字母都是合式公式.

2) 若 $\mathscr{A},\mathscr{B}$ 是合式公式，则$(\neg\mathscr{A})$，$(\mathscr{A}\wedge\mathscr{B})$也是合式公式.

3) 若 $\mathscr{A}$ 是合式公式，则$\Diamond\mathscr{A}$ 也是合式公式.

4) 合式公式仅由 1)～3)构成.

(3) **定义**(联结词转换的定义)

1) $\mathscr{A}\vee\mathscr{B}\triangleq\neg(\neg\mathscr{A}\wedge\neg\mathscr{B})$.

2) $\mathscr{A}\prec\mathscr{B}\triangleq\neg\Diamond(\mathscr{A}\wedge\mathscr{B})$. $(\Box(\mathscr{A}\rightarrow\mathscr{B}))$.

3) $\mathscr{A}=\mathscr{B}\triangleq(\mathscr{A}\prec\mathscr{B})\wedge(\mathscr{B}\prec\mathscr{A})$.

4) $\Box\mathscr{A}\triangleq\neg\Diamond\neg\mathscr{A}$ $(\neg\mathscr{A}\triangleq\neg M\neg\mathscr{A})$.

注 联结词"$\prec$"称为"严格蕴含词"(strict implication),联结词"$=$"称为"严格等价"(strict equivalence).

(4) **公理集**(axiom)

用公理模式给出,其中 $\mathscr{A},\mathscr{B},\mathscr{C}$ 是 S1 中任意的合式公式.

AS1. 1 $\mathscr{A}\wedge\mathscr{B}\prec\mathscr{B}\wedge\mathscr{A}$.

AS1. 2 $\mathscr{A}\wedge\mathscr{B}\prec\mathscr{A}$.

AS1. 3 $\mathscr{A}\prec\mathscr{A}\wedge\mathscr{A}$.

AS1. 4 $(\mathscr{A}\wedge\mathscr{B})\wedge\mathscr{C}\prec\mathscr{A}\wedge(\mathscr{B}\wedge\mathscr{C})$.

AS1. 5 $((\mathscr{A}\prec\mathscr{B})\wedge(\mathscr{B}\prec\mathscr{C}))\prec(\mathscr{A}\prec\mathscr{C})$.

AS1. 6 $\mathscr{A}\wedge(\mathscr{A}\prec\mathscr{B})\prec\mathscr{B}$.

(5) **推理规则(变换规则** rule of inference/rule of transformation)

1) 等价变换规则(标准逻辑).

2) 严格等价变换规则:$\vdash\mathscr{A}$, $\vdash\mathscr{C}=\mathscr{D}$,则 $\vdash\mathscr{B}$.

其中 $\mathscr{B}$ 是 $\mathscr{A}$ 中所含子公式 $\mathscr{C}$ 被另一个子公式 $\mathscr{D}$ 替换后所得到的新公式.

3) 若 $\vdash\mathscr{A}$, $\vdash\mathscr{B}$,则 $\vdash(\mathscr{A}\wedge\mathscr{B})$.

4) **分离规则**(modus ponens):若 $\vdash\mathscr{A}$, $\vdash(\mathscr{A}\prec\mathscr{B})$,则 $\vdash\mathscr{B}$.

注 (1) 由于模态逻辑是古典逻辑的扩充,所以有关"推演"与"断定"的符号 $\vdash$,完全与古典逻辑相仿,不再赘述.

(2) 此处的分离规则与古典逻辑略有不同,它是在严格蕴含词下成立的,比古典逻辑中的 PM 规则要强.

定义 23. 2. 2 系统 T(系统 M)

(1) 符号(字母)库

命题字母：$P,Q,R,\cdots,P_1,Q_1,R_1,\cdots,P_2,Q_2,R_2,\cdots$

初始联结词：$\neg,\vee$.

辅助符号：括号),(.

模态算子：$\Box(L)$.

(2) 合式公式集(公式集)

1)所有的命题字母都是合式公式.

2)若 $\mathscr{A},\mathscr{B}$ 是合式公式，则$(\neg\mathscr{A})$，$(\mathscr{A}\vee\mathscr{B})$也是合式公式.

3)若 $\mathscr{A}$ 是合式公式，则$\Box\mathscr{A}$ 也是合式公式.

4)合式公式仅由 1)～3)构成.

(3) 定义(联结词转换的定义)

1)$\mathscr{A}\rightarrow\mathscr{B}\triangleq\neg\mathscr{A}\vee\mathscr{B}$.

2)$\mathscr{A}\wedge\mathscr{B}\triangleq\neg(\neg\mathscr{A}\vee\neg\mathscr{B})$.

3)$\mathscr{A}\leftrightarrow\mathscr{B}\triangleq(\mathscr{A}\rightarrow\mathscr{B})\wedge(\mathscr{B}\rightarrow\mathscr{A})$.

4)$\mathscr{A}\prec\mathscr{B}\triangleq\Box(\mathscr{A}\rightarrow\mathscr{B})$.　　$(\neg\Diamond(\mathscr{A}\wedge\mathscr{B}))$.

5)$\mathscr{A}=\mathscr{B}\triangleq((\mathscr{A}\prec\mathscr{B})\wedge(\mathscr{B}\prec\mathscr{A}))$.

6)$\Diamond\mathscr{A}\triangleq\neg\Box\neg\mathscr{A}$.

注　联结词“$\prec$”,“$=$”均与定义 23.2.1 同.

(4) 公理集

用公理模式给出，其中 $\mathscr{A},\mathscr{B},\mathscr{C}$ 是 T 中任意的合式公式.

AT.1　$\mathscr{A}\vee\mathscr{A}\rightarrow\mathscr{A}$.

AT.2　$\mathscr{A}\rightarrow\mathscr{A}\vee\mathscr{B}$.

AT.3　$\mathscr{A}\vee\mathscr{B}\rightarrow\mathscr{B}\vee\mathscr{A}$.

AT.4　$(\mathscr{B}\rightarrow\mathscr{C})\rightarrow((\mathscr{A}\vee\mathscr{B})\rightarrow(\mathscr{A}\vee\mathscr{C}))$.

AT.5　$\Box\mathscr{A}\rightarrow\mathscr{A}$.

AT.6　$\Box(\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\Box\mathscr{A}\rightarrow\Box\mathscr{B})$.

(5) 推理规则(变换规则 rule of inference/rule of transformation)

1) 等价变换规则(标准逻辑).

2) **分离规则**:若 $\vdash\mathscr{A}$, $\vdash\mathscr{A}\to\mathscr{B}$,则 $\vdash\mathscr{B}$.

3) **必然规则**(N):若 $\vdash\mathscr{A}$,则 $\vdash\Box\mathscr{A}$.

注 这里的分离规则要强,即这里的公式 $\mathscr{A}$,$\mathscr{B}$ 是模态系统 T 中的合式公式,其中可以带有模态算子.

模态系统 S1,T 都是较弱的模态系统,有些文献中称系统 T 是最弱的系统,然而 S1 也是较弱的系统,但是系统 S1 并不包含系统 T,同样系统 T 也不包含系统 S1(这里所说"包含"的意思是:若系统 S1 中的定理集 Th(S1)与系统 S2 中的定理集 Th(S2)有关系:$\mathrm{Th}(S1)\supseteq\mathrm{Th}(S2)$,则称系统 S1 包含 S2.)

为了陈述其余的模态系统,首先给出了一个合式公式库与一个推理规则库,在此基础上以统一的方式给出各种不同的系统.

定义 23.2.3 **公式库**中有下述合式公式:

A0 $\Box(\mathscr{A}\to\mathscr{B})\to(\Box\mathscr{A}\to\Box\mathscr{B})$.

A1 $\Box\mathscr{A}\to\mathscr{A}$.

A2 $\Box\mathscr{A}\to\Diamond\mathscr{A}$.

A3 $\Box\mathscr{B}\to(\mathscr{A}\to\Box\Diamond\mathscr{A})$.

A4 $\Box(\mathscr{A}\to\mathscr{B})\to\Box(\Box\mathscr{A}\to\Box\mathscr{B})$.

A5 $\Box\mathscr{A}\to\Box\Box\mathscr{A}$.

A6 $\Box\mathscr{B}\to(\Diamond\mathscr{A}\to\Box\Diamond\mathscr{A})$.

A7 $\Box\mathscr{B}\to\Box(\Diamond\mathscr{A}\to\Box\Diamond\mathscr{A})$ $(\Box\mathscr{B}\to(\Diamond\mathscr{A}\prec\Box\Diamond\mathscr{A}))$.

A8 $\Box(\Diamond(\mathscr{A}\wedge\mathscr{B})\to\Diamond\mathscr{A})$ $(\Diamond(\mathscr{A}\wedge\mathscr{B})\prec\Diamond\mathscr{A})$.

A9 $\Box(\Box(\mathscr{A}\to\mathscr{B})\to\Box(\Box\neg\mathscr{B}\to\Box\neg\mathscr{A}))$

$(\mathscr{A}\prec\mathscr{B})\prec(\neg\Diamond\mathscr{B}\to\neg\Diamond\mathscr{A})$.

A10 $\Diamond\Diamond\mathscr{A}$.

其中 $\mathscr{A}$,$\mathscr{B}$ 均为合式公式.

定义 23.2.4 **推理规则库**中有下述规则:

R1 $\mathscr{A}\to\mathscr{B}/\Box\mathscr{A}\to\Box\mathscr{B}$.

R2　$\Box(\mathscr{A}\to\mathscr{B})/\Box(\Box\mathscr{A}\to\Box\mathscr{B})$.

R3　$\mathscr{A}/\Box\mathscr{A}$.

R4　$/\Box\mathscr{A}$(必然规则)，其中 $\mathscr{A}$ 是古典逻辑中的定理，即 $\vdash\mathscr{A}$ 则 $\vdash\Box\mathscr{A}$.

R5　$\Box\mathscr{A}/\mathscr{A}$.

其中 $\mathscr{A},\mathscr{B}$ 均为合式公式.

注　表达式 $\mathscr{A}\to\mathscr{B}/\Box\mathscr{A}\to\Box\mathscr{B}$ 表示：若 $\vdash\mathscr{A}\to\mathscr{B}$，则 $\vdash\Box\mathscr{A}\to\Box\mathscr{B}$. 余同.

现在把模态系统分列如下：

S1

S2 = S1 + A8

= A0 + A1 + □A0 + □A1 + R2 + R4.

S3 = S1 + A9

= A1 + A4 + □A1 + □A4 + R4.

S4 = S1 + □A5

= M + A5.

S5 = S1 + A7

= M + A6.

S6 = S2 + A10.

S7 = S3 + A10.

S8 = S3 + □A10.

S9 = S3. 5 + A10.

S0. 5° = A0 + R4.

S0. 5 = A0 + A2 + R4.

S2° = A0 + □A0 + R2 + R4 + R5.

S3. 1 = S3 + ◇□A5.

S3. 5 = S3 + A6.

C2 = A0 + R1.

D2＝C2＋A2.

E2＝C2＋A1.

I＝A0＋R3.

M(T)＝I＋A1.

B＝M＋A3.

注 S2°＝A0＋□A0＋R2＋R4＋R5 表示模态系统 S2°是由公理：A0 与□A0(公理 A0 是公式□($\mathscr{A}\to\mathscr{B}$)→(□$\mathscr{A}$→□$\mathscr{B}$)，所以公理□A0 就是□(□($\mathscr{A}\to\mathscr{B}$)→(□$\mathscr{A}$→□$\mathscr{B}$))，即把模态算子□作用于公理 A0 的表达式上. 余同.

由上可知模态逻辑系统是非常丰富的，各个系统的强弱程度也不一样，比如模态系统 S5 是包含 S4 的(即 Th(S5)⊇Th(S4))，但 S1 与 T 却没有这种简单的关系. 下面用图示给出各系统间的包含关系，用 S→S′表示 Th(S)⊆Th(S′).

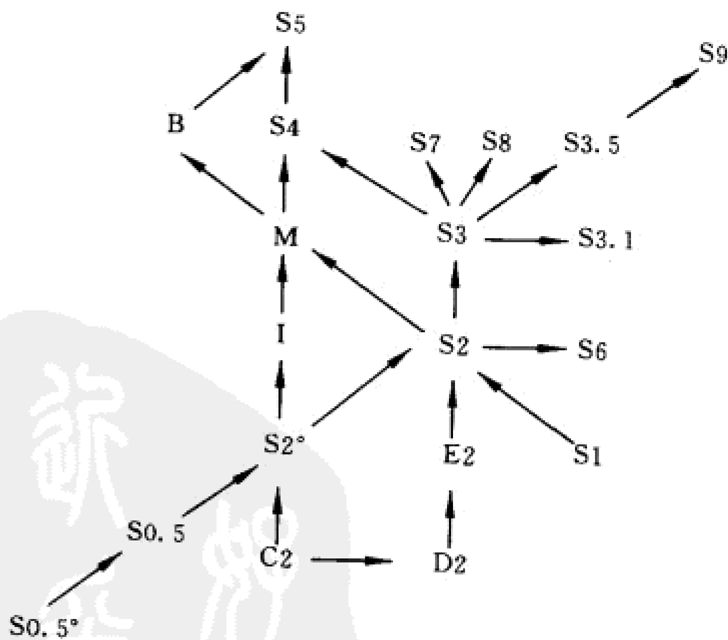


图 23.1

依据各种情况，添加不同的公理，可以得出各种不同的模态系统，尤其是在S4与S5之间，S3与S5之间可以插入各种中介系统，以供人们的需求，限于篇幅不多述.

23.2.2 模态命题逻辑的语义及普效性

古典命题逻辑是二值逻辑系统，系统中每一个公式，当其中命题变量的真假值确定之后，它的真假值也唯一地确定. 但在模态系统中，情况就完全不同了. 这时要考虑所有的可能世界（而不仅仅是一种世界）. 在不同的可能世界中，公式的真值也不尽相同，应该给出它在每一个可能世界中的赋值.

在古典命题逻辑中，一个公式，若对于它的命题变量的任意一组赋值都取值为真，则此公式就是普效式（重言式）. 而在模态系统中，模态公式的普效性，就要考虑到可能世界. 因此必须要用数学结构（模型）给出普效性的严格定义.

定义 23.2.5 称三元组结构 $\mathscr{M}=\langle W,R,v\rangle$ 为**标准模型**（standard model）的充要条件是：

（1）W 是一个非空集合.

（2）R 是 W 上的二元关系.（$R\subseteq W\times W$）.

（3）v 是真值赋值.

其中称 W 是**可能世界集**（possible world），R 是可能世界间的二元关系，称为**可达关系**（accessibility relation）.

定义 23.2.6 设 $\mathscr{M}=\langle W,R,v\rangle$ 是标准模型，赋值 v 定义如下：

（1）对于任意的命题变元 p_j，任意的可能世界 $w_i\in W$：

$$v(p_j,w_i)=\top \text{ 或 } v(p_j,w_i)=\bot.$$

（2）对于任意的合式公式 $\mathscr{A}$，任意的可能世界 $w_i\in W$：

$$v(\neg\mathscr{A},w_i)=\begin{cases}\top, \text{当 } v(\mathscr{A},w_i)=\bot\text{时},\\ \bot, \text{当 } v(\mathscr{A},w_i)=\top\text{时}.\end{cases}$$

（3）对于任意的合式公式 $\mathscr{A},\mathscr{B}$，任意的可能世界 $w_i\in W$：

$$v(\mathscr{A}\vee\mathscr{B},w_i)=\begin{cases}\top\text{，当 } v(\mathscr{A},w_i)=\top \text{ 或 } \\ \qquad v(\mathscr{B},w_i)=\top \text{ 时，}\\ \bot\text{，其他情形.}\end{cases}$$

(4) 对于任意的合式公式 $\mathscr{A},\mathscr{B}$，任意的可能世界 $w_i\in \boldsymbol{W}$：

$$v(\mathscr{A}\wedge\mathscr{B},w_i)=\begin{cases}\top\text{，当 } v(\mathscr{A},w_i)=\top \text{ 且 } v(\mathscr{B},w_i)=\top\text{，}\\ \bot\text{，其他情形.}\end{cases}$$

(5) 对于任意的合式公式 $\mathscr{A},\mathscr{B}$，任意的可能世界 $w_i\in \boldsymbol{W}$：

$$v(\mathscr{A}\rightarrow\mathscr{B},w_i)=\begin{cases}\top\text{，当 } v(\neg\mathscr{A},w_i)=\top \text{ 或 } v(\mathscr{B},w_i)=\top\text{时，}\\ \bot\text{，其他情形.}\end{cases}$$

(6) 对于任意的合式公式 $\mathscr{A}$，任意的可能世界 $w_i\in \boldsymbol{W}$：

$$v(\Box\mathscr{A},w_i)=\begin{cases}\top\text{，对任意的 } w_j\in \boldsymbol{W} \text{ 且 } w_iRw_j\text{：} v(\mathscr{A},w_j)=\top\text{时，}\\ \bot\text{，其他情形.}\end{cases}$$

现在给出一个合式公式在某个系统中是普效的(有效的)严格定义.

定义 23.2.7 设 $\mathscr{A}$ 是系统中的合式公式，若对于该系统的任意模型 $\mathscr{M}=\langle \boldsymbol{W},R,v\rangle$ 以及任意的 $w_i\in \boldsymbol{W}$，均有 $v(\mathscr{A},w_i)=\top$，则称 $\mathscr{A}$ 在该系统中是**普效的**(有效的).

一般情形，在标准模型下，对关系 R 不加任何限制时的系统，下列公式

$\Box(\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\Box\mathscr{A}\rightarrow\Box\mathscr{B})$，　　(公理 A0)

$\Diamond\mathscr{A}\leftrightarrow\neg\Box\neg\mathscr{A}$，

$\Box\mathscr{A}\leftrightarrow\neg\Diamond\neg\mathscr{A}$，

以及推理规则中的必然规则(N)：$/\mathscr{A}$，则$/\Box\mathscr{A}$，都是有效的，但是公理 A1，A5，A6 就不是在所有的标准模型中都能成立. 有下面的结论.

定理 23.2.8 设 $\mathscr{M}=\langle \boldsymbol{W},R,v\rangle$ 是标准模型.

(1) 若关系 R 是自反的，则公理 A1 成立.

(2) 若关系 R 是传递的，则公理 A5 成立.

(3) 若关系 R 是欧几里得的，则公理 A6 成立.（R 是欧几里得的：对于任意的 w_i, w_j, w_k，若 $w_i R w_j$ 且 $w_i R w_k$，则 $w_j R w_k$；换言之，R 是欧几里得几何中的“平行”关系.）

因此可知，A1 是 T 有效的、S4 有效的与 S5 有效的；A5 是 S4 有效的与 S5 有效的；A6 是 S5 有效的.

随着对标准模型中，关系 R 的限制不同，就产生不同的模态系统，见表 23.1.

表 23.1

模态命题逻辑	对 R 的限制
T	自反关系
S4	自反，传递关系
B	自反，对称关系
S5	等价关系或自反，欧几里得的

23.2.3 模态谓词逻辑系统

在古典谓词逻辑系统中添加模态算子，就可以构成与模态命题逻辑系统相应的模态谓词逻辑系统. 为简便计，把古典谓词逻辑系统记作 LPC，相应的模态谓词系统就分别记作：

LPC＋B1，LPC＋T，LPC＋S4（有些文献中则分别记作 B_1Q，TQ，S_4Q…）

模态谓词逻辑系统是在模态形式语言 $\mathscr{L}^m$（而 $\mathscr{L}^m$ 是在形式语言 $\mathscr{L}$（参见 22.5.1 节）中添加模态词□得到的）中表达的.

$$\mathrm{Alp}(\mathscr{L}^m) = \mathrm{Alp}(\mathscr{L}) + \{\Box\}.$$

$$\mathrm{Term}(\mathscr{L}^m) = \mathrm{Term}(\mathscr{L}).$$

$\mathrm{Form}(\mathscr{L}^m)$ 定义如下：

(1) $\mathrm{Term}(\mathscr{L}^m) \subseteq \mathrm{Form}(\mathscr{L}^m)$.

(2) 若 $\mathscr{A} \in \mathrm{Form}(\mathscr{L}^m)$，则 $(\neg \mathscr{A})$，$\Box\mathscr{A} \in \mathrm{Form}(\mathscr{L}^m)$.

(3) 若 $\mathscr{A},\mathscr{B}\in \text{Form}(\mathscr{L}^m)$，则 $\mathscr{A}\to\mathscr{B}\in \text{Form}(\mathscr{L}^m)$.

(4) $\mathscr{A}\in \text{Form}(\mathscr{L}^m)$，$x$ 是变元，则 $(\forall x)\mathscr{A}\in \text{Form}(\mathscr{L}^m)$.

(5) 公式仅由(1) ～(4) 所规定.

详言之

$\text{LPC}+\text{T}=\text{Alp}(\mathscr{L}^m)+\text{Form}(\mathscr{L}^m)+\text{Axiom}(\mathscr{L})+\text{Rule}(\mathscr{L})+\text{T}.$

$\text{LPC}+\text{B}=\text{Alp}(\mathscr{L}^m)+\text{Form}(\mathscr{L}^m)+\text{Axiom}(\mathscr{L})+\text{Rule}(\mathscr{L})+\text{B}$

以此类推，不赘述(参看 22.5.1 节).

在模态逻辑中，由于引入了模态算子，增加了系统的描述能力(或表达能力)，但同时也增加了系统的复杂性. 在模态命题逻辑中，模态算子与逻辑联结词之间的关系，已如前述. 在模态谓词逻辑中，模态算子与量词之间的关系尤为突出. 一般情况，人们希望对于任意的合式公式能有

$$\Box(\forall x)\mathscr{A}\Leftrightarrow(\forall x)\Box\mathscr{A}.$$

这就导致下面的 Barcan 公式*，简记作

$$\text{BF}\qquad (\forall x)\Box\mathscr{A}\to\Box(\forall x)\mathscr{A}.$$

已知在系统 LPC+T 中(不用 BF)的定理有：

$$\vdash_{\text{LPC+T}}\Box(\forall x)\mathscr{A}\to(\forall x)\Box\mathscr{A}.$$

$$\vdash_{\text{LPC+T}}\Diamond(\forall x)\mathscr{A}\to(\forall x)\Diamond\mathscr{A}.$$

$$\vdash_{\text{LPC+T}}(\exists x)\Box\mathscr{A}\to\Box(\exists x)\mathscr{A}.$$

由于定理 $\vdash_{\text{LPC+T}}\Box(\forall x)\mathscr{A}\to(\forall x)\Box\mathscr{A}$ 是 BF 的逆，所以如果承认 BF 是系统中的公理，那么在这个系统中(即系统 LPC+T+BF)就有 $\Box(\forall x)\mathscr{A}\Leftrightarrow(\forall x)\Box\mathscr{A}$.

(即同时有 $\vdash_{\text{LPC+T+BF}}\Box(\forall x)\mathscr{A}\to(\forall x)\Box\mathscr{A}$，及 $\vdash_{\text{LPC+T+BF}}(\forall x)\Box\mathscr{A}\to\Box(\forall x)\mathscr{A}$).

此外，还可知 BF 在 LPC+S4 中不是定理，但它在 LPC+S5 中是可证的，更甚者在系统LPC+T+BF中下面的公式是可证的

---

* 此公式由 Ruth C. Barcan 提出.

$$(\forall x)\Box(\mathscr{A}\to\mathscr{B})\to\Box((\forall x)\mathscr{A}\to(\forall x)\mathscr{B}),$$

即

$$(\forall x)(\mathscr{A}\prec\mathscr{B})\to((\forall x)\mathscr{A}\prec(\forall x)\mathscr{B}).$$

这正是人们所期待的.

最后介绍模态逻辑的语义.

模态谓词逻辑语义是把模态命题逻辑与古典谓词逻辑的语义结合而成.

模态谓词逻辑的模型是一个四元组$\langle W,R,D,v\rangle$. 其中W是可能世界集(非空),R是W上的二元关系,D是个体域(非空),v是赋值.

(1) 对于系统中的个体变元(量)x,赋予D中的一个元素:$v(x)=u,u\in D$.

(2) 对于每一个u元谓词F,$v(F)=\{\langle u_1,u_2,\cdots,u_n,w_i\rangle \mid u_i(i=1,2,\cdots,n)\in D,w_i\in W\}$.

(3) 对于任意的合式公式$\mathscr{A}$,任意的可能世界$w_i\in W$,赋予值$v(\mathscr{A},w_i)$如下:

1) 若F是u元谓词,则

$$v(F(x_1,\cdots,x_n),w_i)=\begin{cases}\bot,若\langle v(x_1),\cdots,v(x_n),w_i\rangle\in v(F);\\ \top,若\langle v(x_1),\cdots,v(x_n),w_i\rangle\notin v(F).\end{cases}$$

2) 对于任意的合式公式$\mathscr{A}$,任意的$w_i\in W$:

$$v(\neg\mathscr{A},w_i)=\begin{cases}\top,若\ v(\mathscr{A},w_i)=\bot;\\ \bot,若\ v(\mathscr{A},w_i)=\top.\end{cases}$$

3) 对任意的合式公式$\mathscr{A},\mathscr{B}$,任意的$w_i\in W$:

$$v(\mathscr{A}\vee\mathscr{B})=\begin{cases}\top,若\ v(\mathscr{A},w_i)=\top或\ v(\mathscr{B},w_i)=\top;\\ \bot,若\ v(\mathscr{A},w_i)=\bot且\ v(\mathscr{B},w_i)=\bot.\end{cases}$$

4) 对任意的合式公式$\mathscr{A}$,任意的个体变元,任意的$w_i\in W$,令v'是与v几乎相等的赋值(见定义22.3.8):

$$v((\forall x)\mathscr{A},w_i)=\begin{cases}\top, 若对所有的 v' 都有 v'(\mathscr{A},w_i)=\top;\\ \bot, 其他情形.\end{cases}$$

5）对任意的合式公式 $\mathscr{A}$，任意的 $w_i\in W$：

$$v(\Box\mathscr{A},w_i)=\begin{cases}\top, 若对所有的 w_j, w_iRw_j,\\ \quad 则有 v(\mathscr{A},w_j)=\top;\\ \bot, 其他情形.\end{cases}$$

在 LPC＋T＋BF 模型中，关系 R 要求是自反的，在 LPC＋S4＋BF 模型中，关系 R 要求是自反的与传递的；在 LPC＋S5 中关系 R 要求是等价的.

定义 23.2.9

(1) 任意的合式公式 $\mathscr{A}$ 是 LPC＋T＋BF **有效的**充要条件是对于每一个 LPC＋T＋BF 模型 $\langle W,R,D,v\rangle$，以及任意的 $w_i\in W$ 均有 $v(\mathscr{A},w_i)=\top$.

(2) 任意的合式公式 $\mathscr{A}$ 是 LPC＋S4＋BF **有效的**充要条件是对于每一个 LPC＋S4＋BF 模型 $\langle W,R,D,v\rangle$，以及任意的 $w_i\in W$ 均有 $v(\mathscr{A},w_i)=\top$.

(3) 任意的合式公式 $\mathscr{A}$ 是 LPC＋S5 **有效的**充要条件是对于每一个 LPC＋S5 模型 $\langle W,R,D,v\rangle$，以及任意的 $w_i\in W$ 均有 $v(\mathscr{A},w_i)=\top$.

关于其他模型，情况完全类似.

23.3 多值逻辑

古典逻辑的语义解释只使用两个真值. 如果在所考虑的逻辑系统里，一个命题可以取得多于两个不同的真值，则此系统称为多值逻辑.

多值逻辑的历史可以追溯到 Aristotle，20 世纪初，苏格兰人 H. MacColl(1837—1909)，美国人 C. S. Peirce(1839—1914)以及

前苏联人 N. A. Vasilev(1880—1940)都研究过多值逻辑. 然而最早较为系统地研究多值逻辑系统则是在 20 世纪 20 年代始自波兰逻辑学家 J. Łukasiewicz 和美国逻辑学家 E. L. Post.

前苏联逻辑学家 D. A. Bochvar 由于想克服语义悖论,提出了 3-值逻辑系统 B,美国数学家 S. Kleene 由于研究数学中不可判定问题,构造了 3-值逻辑系统 K_3,美籍法国逻辑学家 H. Reichenbach 从量子力学的角度出发,构造了相应的 3-值量子逻辑 R_3.

此后人们继续进行理论探讨,试图建立多值逻辑的一般理论,建立各种完备的多值逻辑演算,研究各种演算方法,规则和性质,研究各种不同系统之间的关系以及多值逻辑与古典逻辑之间的关系. 但多限于理论研究,20 世纪 70 年代以后,由于计算机技术突飞猛进的发展,使得多值逻辑的理论及应用得到了更快的发展.

3-值逻辑是最简单的多值逻辑,也是最重要的逻辑系统,以 3-值逻辑系统为背景可以更深入地了解多值逻辑系统的理论与应用. 目前,多值逻辑对数字电路系统的应用还不如古典逻辑理论成熟,这是由于多值逻辑电路的复杂性和电路实现的困难性. 尽管如此,多值逻辑系统已经应用于故障检测、容错计算、故障安全、软件设计、人工智能、模式识别、机器学习等方面,很可能未来的逻辑系统是古典逻辑系统与多值逻辑系统组成的混合系统.

23.3.1 3-值命题逻辑

在古典逻辑中,任何命题都确定地为真或为假. 3-值逻辑则使用第三个真值. 这第三个真值在某些解释中表示以一定方式介于真和假之间的一个中间值. 现在已有许多关于第三个真值的直观解释,它们在各种观点下都是合理的.

有许多 3-值命题逻辑系统,但是我们只着重考察下述重要的 4 种,即 Kleene, Łukasiewicz, Bochvar 以及 Reichenbach 的

3-值逻辑.

1. Kleene 3-值逻辑系统 K_3

这种逻辑系统是想描述未确定的数学命题. 第 3 个真值的直观意义是表示“未定义(u)”,把它赋值到某个合式公式时并不是想说明该公式既不真也不假,而是想要表示一种未知的状态. 因此一个命题可以有三个真值: 真(t),假(f)和中间值(u)(未定义).

Kleene 3-值命题逻辑的联结词与古典逻辑相同,它的真值表由古典逻辑的真值表扩充而成(见表 23.2).

表 23.2

A	$\neg A$
t	f
f	t
u	u

$A \wedge B$		B t	f	u
	t	t	f	u
A	f	f	f	f
	u	u	f	u

$A \vee B$		B t	f	u
	t	t	t	t
A	f	t	f	u
	u	t	u	u

$A \to B$		B t	f	u
	t	t	f	u
A	f	t	t	t
	u	t	u	u

$A \leftrightarrow B$		B t	f	u
	t	t	f	u
A	f	f	t	u
	u	u	u	u

Kleene 3-值逻辑系统按下列原则建立:

(1) 3 个真值按真值性减小次序排列为: t,u,f.

(2) 命题与其否定式的取值有“镜象”的特点(即原命题取值为 t 时,其否定式取值为 $f = \neg t$).

(3) 合取式与析取式的取值如下:

$$A \wedge B = \min(A, B);$$

$$A \vee B = \max(A, B).$$

(4) 下列公式成立：

$$A \to B = \neg A \vee B;$$

$$A \to B = (A \to B) \wedge (B \to A).$$

(5) 古典逻辑中的排中律，在 K_3 中不再成立. 事实上，公式 $A \vee \neg A$ 在 $A = u$ 时其值仍为 u.

(6) 古典逻辑中的重言式在 K_3 中未必仍是重言式，例如公式 $A \to A$ 是古典逻辑中的重言式，但在 K_3 中它的值并非恒取 t 值.

(7) 古典逻辑中的矛盾律 $\neg(P \wedge \neg P)$ 在 K_3 中也不成立.

2. Łukasiewicz 3-值逻辑系统 Ł$_3$

这种逻辑系统是发展了 Kleene 3-值逻辑系统，它是用来处理未来可能发生事件的命题. 例如命题：“明年 12 月 21 日中午，我将在华沙”，他认为在讲这句话时，它既不真也不假，而只是可能. 因此，一个命题可以有 3 个真值：真(t)，假(f)和中间值(i).

Łukasiewicz 3-值逻辑的联结词也与古典逻辑基本相同，它的真值表也是由古典逻辑的真值表扩充而成(见表 23.3).

表 23.3

A	$\neg A$
t	f
f	t
i	i

$A \wedge B$		B: t	f	i
A	t	t	f	i
	f	f	f	f
	i	i	f	i

$A \vee B$		B: t	f	i
A	t	t	t	t
	f	t	f	i
	i	t	i	i

$A \to B$		B: t	f	i
A	t	t	f	i
	f	t	t	t
	i	t	i	t

$A \leftrightarrow B$		B: t	f	i
A	t	t	f	i
	f	f	t	i
	i	i	i	t

Łukasiewicz 3-值逻辑按下列原则建立：

(1) 3 个真值按照真值性减小次序排列为 t,i,f.

(2) 命题与其否定式的取值，有"镜象"的特性.

(3) 合取式与析取式的取值如下：

$$A \wedge B = \min(A,B);$$

$$A \vee B = \max(A,B).$$

(4) 公式 $A \to B$ 与公式 $\neg A \vee B$ 的值基本相同. 但有例外，即蕴含式 $A \to A$ 的值为 t. 因此，公式 $A \to B$ 与公式 $\neg A \vee B$ 在 $A = B = \mathrm{i}$ 时是不相同的.

(5) 公式 $A \leftrightarrow B = (A \to B) \wedge (B \to A)$.

(6) 古典逻辑中的排中律与矛盾律在 $Ł_3$ 中不成立.

注 (1) $Ł_3$ 与 K_3 的联结词在条件式与双条件式上是不同的. 按照 Łukasiewicz 的解释，当前提和结论均为不确定(i)时，条件式与双条件式的值都是真(t). 因此 $Ł_3$ 与 K_3 是不同的，但 $Ł_3$ 中同一律是成立的.

(2) Łukasiewicz 3-值逻辑是由考虑未来可能发生的命题中得到启发，在 $Ł_3$ 中这种命题不但是既不真又不假，而且在某种意义上说，它是不确定的，不但不知道它的真值，甚至它根本就没有真值. 因此 i 的解释不同于 u 的解释：赋值 u 表示"真值空缺"，而赋值 i 表示命题不能被赋予真值或假值，或它本身就没有真假值.

3. Bochvar 3-值逻辑系统 B

这是另一种重要的 3-值逻辑系统，它是由 D. A. Bochvar 在 1939 年提出，他把 $Ł_3$ 中的中间值(i)解释为"含有某种不可判定的成份."

Bochvar 3-值逻辑与命题的语义悖论有关. 例如：命题："这句话是假的". 对这样的话，如果这句话是真的，则它必定是假的(因为命题本身已说明：这句话是假的.)；如果这句话是假的，则

它必定是真的．这样的命题在古典逻辑中是“排斥”的，是不去处理的．但 Bochvar 认为这种命题既不为真也不为假，而是“自相矛盾的”或“无意义”的；因此在 Bochvar 3-值逻辑系统中，除了真假二值以外的第 3 个真值就是 m（“无意义”）．系统 B 的真值表如表 23.4.

表 23.4

A	$\neg A$
t	f
f	t
m	m

$A\wedge B$		B: t	f	m
A	t	t	f	m
	f	f	f	m
	m	m	m	m

$A\vee B$		B: t	f	m
A	t	t	t	t
	f	t	f	m
	m	t	m	m

$A\rightarrow B$		B: t	f	m
A	t	t	f	m
	f	t	t	m
	m	m	m	m

$A\leftrightarrow B$		B: t	f	m
A	t	t	f	m
	f	f	t	m
	m	m	m	m

Bochvar 3-值逻辑按下列原则建立：

(1) 3 个真值按真值性减小次序排列为 t，f，m.

(2) 命题与其否定式的否定与 $Ł_3$ 同.

(3) 合取式的定义与 K_3，$Ł_3$ 均不相同.

(4) 公式：$A\vee B=\neg(\neg A\wedge\neg B)$，

$A\rightarrow B=\neg(A\wedge\neg B)$，

$A\leftrightarrow B=(A\rightarrow B)\wedge(B\rightarrow A)$，

在 Bochvar 3-值逻辑系统中成立.

(5) 古典逻辑中的排中律及矛盾律在 B 中不再成立.

(6) 为了加强与古典逻辑的联系，Bochvar 在系统 B 中还同

时引进了“外部”联结词(因此系统 B 中原先定义的联结词就称为“内部”联结词).“外部”联结词的真值表如表 23.5.

表 23.5

P	$\urcorner P$
t	f
f	t
m	t

$P \wedge\!\!\wedge Q$		Q: t	f	m
	t	t	f	f
P	f	f	f	f
	m	f	f	f

$P \vee\!\!\vee Q$		Q: t	f	m
	t	t	t	t
P	f	t	f	f
	m	t	f	f

$P \Rightarrow Q$		Q: t	f	m
	t	t	f	f
P	f	t	t	t
	m	t	t	t

$P \Leftrightarrow Q$		Q: t	f	m
	t	t	f	f
P	f	f	t	t
	m	f	t	t

不难看出,由表 23.5 定义的真值函数是一种 3—2 运算.换言之,它是从基本命题的 3 个真值,可以得出运算式的两个真值,因此系统 B 与古典逻辑系统有一部分是相同的,在某种意义上,系统 B 包含了古典逻辑系统.

相对于“内部”联结词而言,“外部”联结词有些优点.例如,公式 $P \wedge \neg P$ 不一定常假(因为当 $P=\mathrm{m}$ 时,它也取值 m),但公式 $P \wedge\!\!\wedge \urcorner P$则常假,且命题 P 与 $\urcorner P$ 之一是常假的.

同样,公式 $P \vee \neg P$ 不是重言式,但 $P \vee\!\!\vee \urcorner P$ 却是重言式.公式 $P \leftrightarrow P$ 不是重言式,但 $P \Leftrightarrow P$ 却是重言式.

4. Reichenbach 3-值量子逻辑系统 R

Reichenbach 曾指出“构造一种 3 值逻辑,也就是说,具有一个不确定的中间值的逻辑是可能的.其中,任意命题的值可以是真或假,或者是不确定的”.为了给量子力学构造一种严格简明的

语言，而且在逻辑结构上可以适用于微观世界的特殊化，他在1942年提出了3-值量子逻辑系统R，扩充了古典逻辑系统的联结词，重新定义，内容十分丰富的逻辑联结词(见表23.6). 它有三种"否定词"，三种"蕴含词"和两种"等值词".

表 23.6

A	$\sim A$	$\bar{A}$	$-A$
t	i	i	f
i	f	t	i
f	t	t	t

在古典逻辑中，"真"的否定式是"假"，"假"的否定式是"真". 在量子逻辑中这种简单的"非此即彼"的排中律是不成立的，因此系统R中有三种"否定词"，否定词"～"称为**循环否定**，它的取值规律是依顺序t,i,f进行循环的. 否定词"－"称为**直接否定**，它与系统Ł_3中的否定词¬类似. 否定词"－"称为**完全否定**，它是系统R所特有的.

其他的联结词真值表见表23.7.

注 (1) 由表23.7中可以看出，系统R中的联结词∧，∨，⊃，≡，与系统Ł_3中的联结词∧，∨，→，↔的真值表完全相同.

(2) 系统R中的联结词∧(有时记作·)，与联结词∨分别称作"合取"与"析取". 系统R中的联结词⊃，→，∋分别称作**标准蕴含**，**选择蕴含**与**准蕴含**. 其中的联结词≡，≣分别称为**标准等价**与**选择等价**. Reichenbach在系统R中增加的"新"的运算，都是出于量子力学的特殊需要.

(3) Reichenbach在系统R中引进的第三个真值(不确定值)乃是由于量子力学观测语言的概率特征，使预言个别事件是否发

生具有不确定性，为了刻画这个事实，他才引进了“不确定值”，作为观测之外的值. 而从逻辑的角度看，“不确定值”恰好是不确定的逻辑状态所具有的真值.

表 23.7

$A \wedge B$		B		
		t	f	i
A	t	t	f	i
	f	f	f	f
	i	i	f	i

$A \vee B$		B		
		t	f	i
A	t	t	t	t
	f	t	f	i
	i	t	i	i

$A \supset B$		B		
		t	f	i
A	t	t	f	i
	f	t	t	t
	i	t	i	t

$A \rightarrow B$		B		
		t	f	i
A	t	t	f	f
	f	t	t	t
	i	t	t	t

$A \ni B$		B		
		t	f	i
A	t	t	f	i
	f	i	i	i
	i	i	i	i

$A \equiv B$		B		
		t	f	i
A	t	t	f	i
	f	f	t	i
	i	i	i	t

$A \equiv B$		B		
		t	f	i
A	t	t	f	f
	f	f	t	f
	i	f	f	t

(4) 由于在系统 R 中，引入了第三真值“不确定”，并且又引进了新的联结词，因此在量子逻辑 R 中，出现了各种带有特异性的重言式，产生了许多在古典逻辑中没有的规律.

1) $A=A.$ （同一律）

2) $A=-(-A)=--A.$ （双重否定律）

3) $A=\sim(\sim(\sim A))=\sim\sim\sim A.$ （三重否定律）

4) $\overline{A}=\overline{((\overline{\overline{A}}))}=\overline{\overline{\overline{A}}}$*. （双重否定律）

5) $\overline{A}=\sim A\vee\sim\sim A.$

6) $A\vee\sim A\vee\sim\sim A=t.$ （排四律）

7) $A\vee\overline{A}=t$**. （假排中律）

8) $\overline{A\wedge\overline{A}}=f,$

$\overline{A\wedge\sim A}=f,$

$\overline{A\wedge -A}=f.$ （矛盾律）

9) $-(A\wedge B)=-A\vee -B,$

$-(A\vee B)=-A\wedge -B.$ （DeMorgan 律）

10) $A\supset B=-B\supset -A,$

$\overline{A}\rightarrow B=\overline{B}\rightarrow A.$

11) $(A\equiv B)=(A\supset B)\wedge(B\supset A).$

12) $A\rightarrow B=\sim -(\overline{A}\vee B).$

13) $(A\supset\overline{A})\supset\overline{A},$

$(A\rightarrow\overline{A})\rightarrow\overline{A}.$

23.3.2 多值命题逻辑

在逻辑系统中，当命题的真值可以取得三值或三值以上，甚至于无穷多值（包括可数无穷或不可数无穷）时，统称为多值逻辑.

---

* 这个双重否定律是对 $\overline{A}$ 而言，它不是直接有效的；易知由此定律推演不出 $A=\overline{\overline{A}}$，因为 $\overline{A}$ 不能用 A 代替（因为原子命题 A3 取三值，而 $\overline{A}$ 仅能取两个真值）.

** 注意，这条规律不是排中律，因为 $\overline{A}$ 不完全与古典逻辑中的"非 A"一致；A 与 $\overline{A}$ 的取值也有所不同.

现着重介绍Łukasiewicz与Post的多值逻辑系统，模糊逻辑将在下一节介绍.

1. Łukasiewicz的多值逻辑

对于多值逻辑，其命题的真值，常常采用数字化的办法来表示；因此对于任意的命题 p，我们用 $|p|$ 表示它的真值，一般情况下 $|p|$ 可以是自然数、有理数或是实数.

从Łukasiewicz的系统 $Ł_3$ 作进一步的扩充，就可以得到多值逻辑系统 $Ł_n$，$Ł_{\aleph_0}$ 甚至于 $Ł_{\aleph}$（在某种意义上说模糊逻辑系统也是一种特殊的 $Ł_{\aleph}$）.

首先介绍 $Ł_n$.

定义 23.3.1 多值逻辑系统 $Ł_n$ 是代数系统

$$\langle V;\neg,\rightarrow\rangle$$

以逻辑联结词 $\neg$ 与 $\rightarrow$ 为初始联结词，定义如下：

$|\neg p|=1-|p|$.

$|p\wedge q|=\min(|p|,|q|)$.

$|p\vee q|=\max(|p|,|q|)$.

$$|p\rightarrow q|=\begin{cases}1, & \text{当}|p|\leqslant|q|,\\ 1-|p|+|q|, & \text{当}|p|>|q|.\end{cases}$$

$p\vee q=(p\rightarrow q)\rightarrow q$.

$p\wedge q=\neg(\neg p\vee\neg q)$.

$p\leftrightarrow q=(p\rightarrow q)\wedge(q\rightarrow p)$.

系统 $Ł_n$ 的真值分布如表23.8及图23.2.

注 23.3.2 由上述的定义及图、表可以看出系统 $Ł_n$ 有下述特点：

(1) 若把1与t(真)对应，0与f(假)对应，则 $Ł_2$ 与古典逻辑系统一致.

(2) 若把 1 与 t(真)对应，$\frac{1}{2}$ 与 i(中间值)对应，0 与 f(假)对应，则 $Ł_3$ 就是 Łukasiewicz 3-值逻辑系统.

表 23.8

n	分　　点	(真　值)
2	$\frac{0}{1},\frac{1}{1},$	$(0,1)$
3	$\frac{0}{2},\frac{1}{2},\frac{2}{2},$	$\left(0,\frac{1}{2},1\right)$
4	$\frac{0}{3},\frac{1}{3},\frac{2}{3},\frac{3}{3},$	$\left(0,\frac{1}{3},\frac{2}{3},1\right)$
5	$\frac{0}{5},\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5},\frac{5}{5},$	
⋮		
n	$\frac{0}{n-1},\frac{1}{n-1},\frac{2}{n-1},\cdots\cdots\frac{n-1}{n-1},$	……

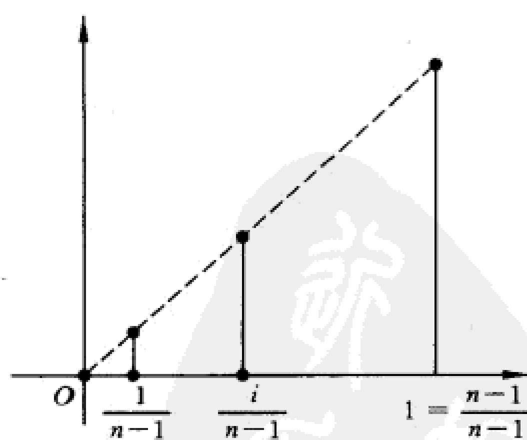


图　23.2

(3) 若把区间[0,1]内所有有理数作为真值，则可以得到 $Ł_3$

的无穷多值扩充，就是 $Ł_{\aleph_0}$，若把区间[0,1]内所有实数作为真值，则可以得到 $Ł_3$ 的另一种扩充 $Ł_{\aleph}$，其中命题的真值集合是一个连续统，这种逻辑又称为连续逻辑.

(4) 必须指出，由于命题真值的分布不同，从系统 $Ł_3$ 进行扩充，可得到许多不同的多值逻辑系统，例如 $Ł_{2n+1}$ 与 $Ł_{[-1,1]}$ 就是这样的系统. 设命题的真值分布是从 $-n$ 到 $n(n\geqslant 2)$ 间的全体整数时，这时的 Łukasiewicz 多值逻辑系统就是 $Ł_{2n+1}$，其中命题的真值有奇数个. 若命题的真值分布是取 -1 到 $+1$ 之间任意实数时，其中 1 表示真，-1 表示假，0 表示中间值，它的初始联结词设为 $\neg$ 与 $\wedge$. 公式的值定义为：

$$|\neg p| = -|p|.$$

$$|p\wedge q| = \min(|p|,|q|,|p|\times|q|)^{①}.$$

其他联结词定义为：

$$p\vee q = \neg(\neg p\wedge\neg q).$$

$$p\rightarrow q = \neg p\vee q.$$

$$p\leftrightarrow q = (p\rightarrow q)\wedge(q\rightarrow p).$$

这样的系统 $Ł_{[-1,1]}$ 也是 $Ł_3$ 的一种扩充.

2. Post 多值逻辑

前述的多值逻辑系统中，否定联结词都有“镜象”的特点. Post 提出了没有这种性质的另一类否定词，在 1921 年他构造出具有 m 个不同真值的多值逻辑系统 P_m.

设命题的真值为 $1,2,\cdots,m$. 其中 1 表示真，m 表示假，中间各值的“真值性”，依次减弱.

定义 23.3.3 多值逻辑系统 P_m 是代数系统.

---

① 其中“×”是实数间的“乘法”.

$$\langle \vee, \overset{m}{\neg}, \overset{m}{\vee} \rangle$$

以逻辑联结词 ¬ 与 ∨ 为初始联结词，定义如下：

否定词的真值表如表 23.9.

表 23.9

P	$\overset{m}{\neg} P$
1	2
2	3
⋮	⋮
$m-2$	$m-1$
$m-1$	m
m	1

$$|p \overset{m}{\vee} q| = \max(|p|, |q|)$$

其他联结词定义如下：

$$p \overset{m}{\wedge} q = \overset{m}{\neg}(\overset{m}{\neg} p \overset{m}{\vee} \overset{m}{\neg} q).$$

$$p \xrightarrow{m} q = \overset{m}{\neg} p \overset{m}{\vee} q.$$

$$p \overset{m}{\leftrightarrow} q = (p \xrightarrow{m} q) \overset{m}{\wedge} (q \xrightarrow{m} p).$$

同样，可以很容易把 Post 的多值逻辑系统 P_m 扩充成无穷多值逻辑；例如，设真值分布为：

$$1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \cdots, \frac{1}{2^k}, \cdots, 0$$

其中各联结词的规则如下：

$$|\neg p| = \begin{cases} 1, & \text{当} |p| = 0, \\ \frac{1}{2}|p|, & \text{当} |p| \neq 0. \end{cases}$$

$$|p \vee q| = \max(|p|, |q|).$$

$$|p \wedge q| = |\neg(\neg p \vee \neg q)|.$$
$$|p \to q| = |\neg p \vee q|.$$
$$|p \leftrightarrow q| = |(p \to q) \wedge (q \to p)|.$$

这个系统称为 $P_{\aleph_0}$. 类似地,可以有 $P_{\aleph}$.

需要特别指出,在 $P_{\aleph_0}$ 与 $P_{\aleph}$ 中没有重言式,但在系统 P_m 中有重言式. 例如

P_2 中,$p \vee \neg p$ 是重言式,

P_3 中,$p \vee \neg p \vee \neg\neg p$ 是重言式,

P_4 中,$p \vee \neg p \vee \neg\neg p \vee \neg\neg\neg p$ 是重言式,

…

P_n 中,$p \vee \neg p \vee \neg\neg p \vee \cdots \vee \underbrace{\neg\neg\neg\cdots\neg}_{(n-1)\text{个}} p$ 是重言式.

23.3.3 多值命题逻辑的重言式与特指真值(特指值)

对于古典逻辑而言,重言式是大家所熟知的,重言式是这样的公式,对于基本命题变元的任意真值赋值,该式的真值永远是真(t). 我们是否可以直截了当的把它移植到多值逻辑系统中去? 看来还需要作适当的修改. 首先考察系统 $Ł_3$,从中可以得到启发.

例 23.3.4 考察公式 $p \to p$, $p \vee \neg p$, $\neg(p \wedge \neg p)$ 的真值. 容易看出在古典逻辑系统中上述三个公式都是重言式. 但是在系统 $Ł_3$ 中,则只有 $p \to p$ 是重言式.

如果我们适当地修改重言式的定义,使得上述三个公式在系统中仍然是重言式,就需要作(在多值逻辑系统中)如下的推广.

在系统 $Ł_3$ 中的三个真值: t,f,i 中,选定其中的 t,i 称为特指真值. 系统 $Ł_3$ 中的公式,对于基本命题变元的任意赋值,该式的真值永取特指真值. 则称它为重言式.

这样处理之后读者可以验证公式 $p \to p$, $p \vee \neg p$, $\neg(p \wedge \neg p)$ 都是重言式(即这些公式的值不是 t,就是 i,绝对不会是 f),不仅

如此，还可以证明，这时古典逻辑系统中的重言式，必定也是系统 $Ł_3$ 中的重言式.

定义 23.3.5 设多值逻辑系统的真值分布为 $1,2,\cdots,M$，而选定真值 s：$1\leqslant s<M$，则称真值 $1,2,\cdots,s$ 是**特指真值**(designated truth value)，$s+1,\cdots,M$ 是**非特指真值**(undesignated truth value).

定义 23.3.6 若多值逻辑系统中的公式，对于基本命题变元的任意赋值，它所取的真值是特指真值(特指值)，则称它为**重言式.**

23.3.4 多值命题逻辑的公理系统

多值命题逻辑的公理系统，其框架完全类似于古典逻辑系统. 它也是在给定符号库、公式集、公理集及推理规则(变换规则)后构成的. 但是由于系统中除"真""假"值外引进了多个真值，因此与二值古典逻辑有所不同.

依传统说法，在多值逻辑系统中常用自然数 $1,2,3,\cdots,s,s+1,\cdots,M$ 由小到大表示命题变量的"真值"，它们代表"真"的程度随数值的大小而逐步递减；数字"1"代表"真"而数值 M 则永远表示"假". 其中 $1,2,\cdots,s$ 称为特指值，而 $s+1,s+2,\cdots,M$ 称为非特指值，而"s"就像是"真""假"值的"分界线". s 与 M 的关系仅仅是 $1\leqslant s<M$(s 永远不能与 M 值相等).

从理论上说，s 与 M 的选取是随意的，但事实上并不如此，它经常是随着理论与应用的需要来选取的.

本节给出由 J. B. Rosser 与 A. R. Turquette 构造的多值命题的逻辑系统. 我们仅仅给出该系统中的公理集如下：

定义 23.3.7 Rosser-Turquette 公理集：

A1 $Q\rightarrow(P\rightarrow Q)$.

A2 $(P\rightarrow(Q\rightarrow R))\rightarrow(Q\rightarrow(P\rightarrow R))$.

A3　$(P\to Q)\to((Q\to R)\to(P\to R))$.

A4　$(J_k(P)\to(J_k(P)\to Q))\to(J_k(P)\to Q), 1\leqslant k<M$.

A5　$\Gamma_I^M(J_i(P)\to Q)\to Q$.

A6　$J_i(P)\to(P), i=1,2,\cdots,s$.

A7　$\Gamma_{k=1}^{\beta}J_{v_k}(P_k)\to J_f(F_i(P_1,\cdots,P_\beta)), i=1,\cdots,b, \beta=\alpha_i$, $f=f_i(P_1,\cdots,P_\beta)$.

注 23.3.8

(1) 上述公理中的 Γ 表示"链式符号".

例如 $\Gamma_3^5 P_i\to Q$ 就表示 $P_5\to(P_4\to(P_3\to Q))$，一般情形把 $\Gamma_{i=u}^{v}P_i\to Q$ 记作 $\Gamma_u^v P_i\to Q$，定义用下述递归规则给出：

$$\Gamma_u^v P_i Q=\begin{cases}Q, & v<u,\\ P_v\to(\Gamma_u^{v-1}P_i\to Q), & v\geqslant u.\end{cases}$$

(2) $f=f_i(p_1,\cdots,p_\beta)$是逻辑函数 $F_i(P_1,\cdots,P_\beta)$的真值.

(3) 逻辑函数 $J_k(P)$的值可以证明为：

$$J_k(P)=\begin{cases}1, & 若\ P=k,\\ M, & 若\ P\neq k.\end{cases}$$

但是逻辑函数的构造比较复杂. 首先，记 $P_1\to P_2$ 为 $F_1(P_1, P_2)$，$\neg P$ 为 $F_2(P)$其值如下：

$$F_1(P_1,P_2)=\max(1,P_2-P_1+1),$$
$$F_2(P)=M-P+1.$$

在此基础上，递归定义函数 $H_i(P)$：

$$H_{t+1}(P)=\begin{cases}F_2(P), & t=0,\\ F_1(P,H_t(P)), & t>0.\end{cases}$$

然后定义 $J_k(P)$如下：

$$J_k(P)=\begin{cases}J_1(F_1(H_I(P)\vee P,H_I(P)\& P)), & k=H_I(k),\\ J_r(H_I(P)), & k>H_I(k).\end{cases}$$

其中

$$1<k<M,$$

而

$$J_1(P)=F_2(H_{M-1}(P)),$$

$$J_M(P)=J_1(F_2(P)).$$

函数 $J_k(\cdot)(1\leqslant k\leqslant M)$的意义，在二值逻辑的背景下可以理解为 $J_1(\cdot),\cdots,J_s(\cdot)$ 相当于恒等函数，$J_{s+1}(\cdot),J_{s+2}(\cdot),\cdots,J_M(\cdot)$相当于否定式，而表达式

$$J_1(\cdot)\vee J_2(\cdot)\vee\cdots\vee\cdots\vee J_M(\cdot)$$

则相当于二值古典逻辑中的表达式 $P\vee\sim P$.

在本节给出的公理系统中，我们给出的初始逻辑函数是 F_i 与 J_k，因此由这些函数构造出的逻辑系统就产生了逻辑函数系的功能完全性(即函数系的完备性)问题.

在多值逻辑理论中，初始逻辑函数系的完全性的判定问题是一个基本而重要的问题，它不仅有理论意义，也有实用价值. 此问题的解决依赖于定出多值函数集 P_k 中所有极大封闭集，Post 和 Яблонский 分别定出了 P_2 与 P_3 中所有极大封闭集，当 $k\geqslant 3$ 时，P_k 中任意极大封闭集已于 1964 年由罗铸楷定出，他指出了下述基本定理：

基本定理 当 $k\geqslant 3$ 时，P_k 中任意极大封闭集必是一个单调函数集 M、T 型集 $T_{E,O}$、保分划函数集 $T_{D'}$、自对偶函数集 S_σ 或线性函数集 L_G.

由此基本结论，只要定出 $T_{D'}$ 中的所有极大封闭集便能得到 P_k 中全部极大封闭集.

但罗铸楷并未定出 $T_{D'}$ 中的全部极大封闭集. 1965 年 Rosenberg 给出了与罗相同的结论，并定出了 $T_{D'}$ 中的所有极大封闭集. 近年来完全 K 值逻辑函数的结构理论有了长足的发展.

附录

中文—外文名词索引

A

B

C

D

E

F

G

H

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

外文—中文名词索引

A

B

C

D

E

F

H

I

J

K

L

M

P

Q

R

S

T

U

V

W

Z



外国人名表

A

Abel,N. H　阿贝尔
Appel,P　阿佩尔
Aristotle　亚里斯多德

B

Barcan,RuthC　巴坎
Bell,E. T　贝尔
Bernays,P　贝尔纳斯
Bernoulli,J　贝努利
Berry,G. G　贝利
Berstein,F　伯恩斯坦
Birkhoff,G　伯克霍夫
Bochvar,D. A　波契瓦尔
Bondy,J. A　邦迪
Boole,G　布尔
Bose,R. C　波塞
Burali-Forti,C　布拉利·弗帝
de Brurijn,N. G　德·布吕恩
Burnside,W　布恩赛德
Burris,S　包利斯

C

Cantor,G　康托

D

E

F



G

H

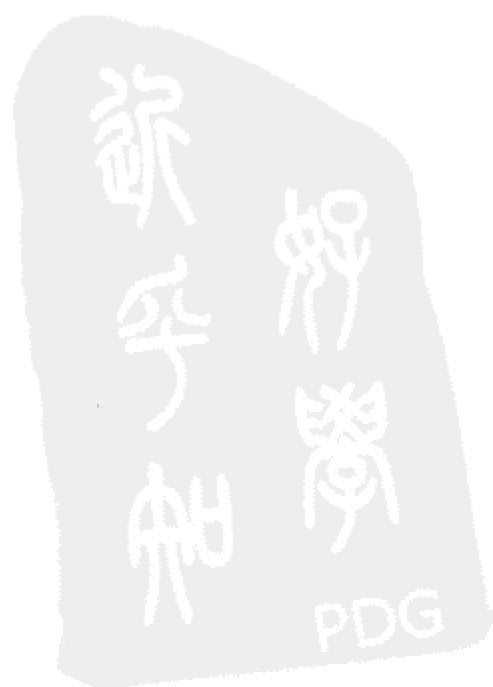
J



K

L

M



N

von Neumann, J　冯·诺依曼
Nicod, J　尼柯
Nörlund, N　罗仑

O

Ore, O　奥尔

P

Peano, G　皮阿罗
Peirce, C. S　皮尔斯
Peterson, W　彼特森
Pólya, G　波利亚
Post, E. L　波斯特

R

Ramsey, F　拉姆赛
Ray-Chaudhuri, D. K　瑞·乔德胡利
Reichenbach, H　莱辛巴赫
Richard, J　里查德
Rosenberg, A　罗森贝尔格
Rosser, J　罗赛尔
Russell, B　罗素

S

Sankappanavar, H. P　桑卡帕纳瓦
Sheffer　谢弗(舍弗)
Skolem, T　斯柯勒姆(斯柯仑)
Socrates　苏格拉底
Steiner, J　斯坦纳

T

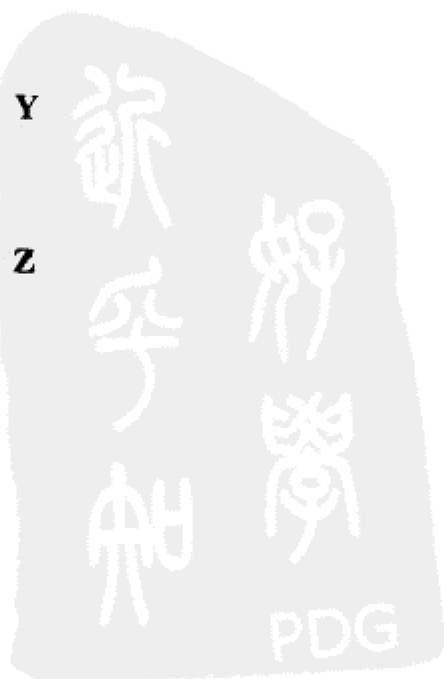
U

V

W

Y

Z



参 考 文 献

1 Berge C. Graphs. North Holland, 1985

2 Birkhoff G and T C Bartee. Modern Applied Algebra. McGraw Hill Book Company, 1970

3 Bollobas B. Extremal Graph Theory. Academic Press, 1978

4 Bondy J A & Murty U S R. Graph Theory with Application. Amer. The Macmillan Press LTD, 1976

5 Bowen K A. Model Theory for Modal logic. Kripke Models for Modal Predicate Calculi. 1978

6 Cohn P M. Universal Algebra. D Reidel Publishing Company, 1981

7 Gould H W. Combinatorial Identities. Morgatown, 1972

8 Grätzer G. Universal Algebra(2nd Ed.)Springer-Verlag, 1979

9 Hamilton A G. Logic for Mathematicians. Cambridge University Press, 1978 (中译本：朱水林译. 数理逻辑. 华东师范大学出版社, 1986)

10 Harary F. Graph Theory. Addison-Wesley, Reading, 1969

11 Harary F & Palmer E M. Graphical Enumeration. AcademicPress, 1973

12 Jacobson N. Lectures in Abstract Algebra I. 1951(中译本：黄像芳译. 抽象代数学, 卷 1. 科学出版社, 1960)

13 Jacobson N. Basic Algebra Ⅰ, Ⅱ. W. H. Freeman and Company, 1974, 1980

14 Kleene S C. Introduction to Metamathematics. van Nostrand, 1952(中译本：莫绍揆译. 元数学导论, 上册(1984), 下册(1985). 科学出版社)

15 Kuratowski K and Mostowski A. Set theory. North-Holland Publishing Company, Amsterdam, 1976

16 MacLane S and G Birkhoff. Algebra (2nd Edition). Macmillan Publishing Company, INC, 1979

17 Maclane S. Categories for the Working Mathematician. Springer-Verlag,1971
18 Moore G H. Zermelós Axiom of Choice Its Origins,Development and Influence. Springer-Verlag,1982
19 Richard , Johnsonbaugh . Discrete Mathematics . Macmillan Publishing Company,1986
20 Riordan J. Combinatorial Identities. John Wiley 82 sons,Inc. ,1968
21 Rosser J B and Turquette A R. Many-valued logics. North-Holland Publishing Company,Amsterdam,1952
22 Rouse Ball WW. Mathematical Recreations and Essays. Macmillan,1962
23 Rubin H and J Rubin. Equivalents of the Axiom of Choice. North-Holland Publishing Company,Amsterdam,1963
24 Stanley Burris and H P Sankappanar. A Course in Universal Algebra. Spring-Verlag,1981
25 Tomescu I. 清华大学离散数学教研组译. 组合学引论,高等教育出版社,1985
26 陈景润. 组合数学简介. 天津科学技术出版社,1988
27 陈昭木. 同调代数初步. 福建科学技术出版社,1984
28 程福长. 同调代数. 广西师范大学出版社,1989
29 方开泰. 均匀设计与均匀设计表. 科学出版社,1994
30 贺昌亭,张同君. 模论讲义. 东北师范大学出版社,1993
31 胡庆平,李丹. 泛代数. 华中理工大学出版社,1993
32 胡冠章. 应用近世代数. 清华大学出版社,1999
33 柯召,魏万迪. 组合论. 科学出版社,1981
34 李乔. 组合数学基础. 高等教育出版社,1993
35 李桃生. 范畴与同调代数. 华中师范大学出版社,1988
36 刘绍学. 环与代数. 科学出版社,1983
37 刘云丰. 布尔代数与逻辑设计,上海教育出版社,1978
38 卢开澄. 组合数学. 清华大学出版社,1989
39 卢开澄. 图论及其应用. 清华大学出版社,1995
40 马克杰. 优美图. 北京大学出版社,1991
41 马振华. 数学逻辑引论. 清华大学出版社,1983



42　马振华. 离散数学导引. 清华大学出版社,1993
43　谢邦杰. 抽象代数学. 上海科学技术出版社,1982
44　邵嘉裕. 组合数学. 同济大学出版社,1991
45　万哲先. 代数和编码. 科学出版社,1980
46　徐利治,蒋茂森,朱自强. 计算组合学. 上海科学技术出版社,1983
47　张永才,张卫. 希尔方法论. 上海科技文献出版社,1993
48　张禾瑞. 近世代数基础. 高等教育出版社,1986



数学科学的成就已成为当今高科技时代进步发展的重要基础，应用数学的发展是科技工业兴旺发达的强有力支柱。为了迎接21世纪的挑战，本手册向您介绍现代应用数学的各个分支，为您在解决科研、数学以及生产实践的各种问题中，提供不可缺少的工具。全书共计六卷：

《运筹学与最优化理论卷》

《现代应用分析卷》

《概率统计与随机过程卷》

《离散数学卷》

《分析与方程卷》

《计算与数值分析卷》

各卷内容自成体系，互相独立，方便读者按需选用。



ISBN 7-302-04565-8

9 787302 045656 >

定价：33.00元